Privacy Impact Assessment Update
for the

E-Verify Program

DHS/USCIS/PIA-030(g)

June 18, 2019

Contact Point
Donald Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
202-272-8030

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS), Verification Division administers an electronic employment verification program called E-Verify. E-Verify is an Internet-based service that allows enrolled participants to confirm the employment eligibility of their newly hired employees and, in some cases, current employees to work in the United States. The USCIS Verification Division is launching new enhancements in order to improve E-Verify by reducing errors and increasing the reliability of the employment eligibility verification process. These enhancements include: (1) a new interconnection to the National Law Enforcement Telecommunications System (NLETS), (2) the use of the Person Centric Entity Resolution microservice, and (3) migration to a cloud-hosted environment. USCIS is publishing an update to this Privacy Impact Assessment (PIA) to describe the collection, use, maintenance, and disclosure of personally identifiable information (PII), as well as the risks associated with these enhancements.

Overview

E-Verify, authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA),[1] is an Internet-based service that allows participating employers to electronically verify the employment eligibility of their new employees to work in the United States. E-Verify is a voluntary program, but employers may be required to participate in E-Verify as a condition of contracting by virtue of entering into a federal contract or subcontract that contains the Federal Acquisition Regulation E-Verify clause. E-Verify participation is also a business licensing or state contracting condition under some state laws. Finally, in some instances, employers may be required to participate in E-Verify because they are part of the Executive Branch or Legislative Branch of government, or as a result of a court order.

E-Verify is a Department of Homeland Security (DHS) program administered by the U.S. Citizenship and Immigration Services (USCIS) Verification Division, and operated in collaboration with the Social Security Administration (SSA). Participating employers use E-Verify to verify the identity and employment eligibility of newly hired employees and, in some cases, current employees, by electronically matching information provided by employees on Form I-9, *Employment Eligibility Verification*,[2] against records available to SSA and DHS.

In addition to SSA, E-Verify is a combined effort with other E-Verify partners, including other DHS components; the Department of State (DOS); and National Law Enforcement Telecommunications System (NLETS); as well as the Department of Justice, Civil Rights Division, Office of Immigrant and Employee Rights Section.[3] E-Verify relies on its partners to

[1] IIRIRA §§ 401-05, codified at 8 U.S.C. § 1324a note.

[2] Form I-9, *Employment Eligibility Verification*, is *available at* https://www.uscis.gov/i-9.

[3] For information on the E-Verify process, see DHS/USCIS/PIA-030 E-Verify Program PIA, *available at* www.dhs.gov/privacy.

verify certain information from the employee or the employer. For example, certain identity and employment authorization information the employee provides on Form I-9 may be compared with SSA and U.S. Customs and Border Protection (CBP) records in order to verify the employee's employment eligibility.

The Immigration Reform and Control Act of 1986 (IRCA) requires that employers verify the employment eligibility of their employees with Form I-9. Employers are responsible for ensuring the employee completes the form and for collecting documentation (e.g., driver's license, birth certificate, passport) from the employee and affirming to the nature of the documentation on the form. Newly hired employees provide their personal information and evidence of identity and employment eligibility to their employer when they complete Form I-9. To confirm the employment eligibility of new hires, employers create a case in E-Verify no later than the third business day after the employee starts work for pay. Form I-9 is the key element of the E-Verify employment eligibility verification process. Employers enter and submit certain information about the employee and the participating company from Form I-9 into E-Verify to initiate a query.

E-Verify electronically compares information provided by the employer to records available to SSA and DHS through automated queries of SSA and DHS systems. A typical E-Verify query occurs by verifying the name, Social Security number (SSN), and date of birth against the SSA's Numident system.[4] E-Verify uses the Verification Information System (VIS), which is a composite information system incorporating data from various databases and functions as the underlying information technology that supports E-Verify. E-Verify uses VIS as the transactional database to verify the information provided by the employee against data from DHS-accessed federal records and state Department of Motor Vehicle Administrations (MVA). This verification provides information permitting the employer to confirm an employee's eligibility to work in the United States. When a non-U.S. citizen is queried, E-Verify displays a match of the name, date of birth, and document information (e.g., Employment Authorization Document or Form I-94, *Arrival-Departure Record*) against other DHS-accessed databases.

If the automated query does not immediately result in an Employment Authorized response from E-Verify, the case is then automatically sent to E-Verify's Status Verification Operations (SVO) division for a manual confirmation of the employee's employment eligibility. SVO has up to three business days to attempt to verify the employee's employment eligibility by manually reviewing the information submitted by the employer with information in DHS-accessed databases. SVO is trained to evaluate the information provided by the employee against the various DHS-accessed databases. If SVO is able to confirm employment eligibility with the information

[4] The Numident file is a record of applications for Social Security numbers. The process of verifying information against SSA's Numident is unchanged as E-Verify continues to verify information via the Verification Information System. *See* 60-0058, Master Files of Social Security Number (SSN) Holder and SSN Applications, 75 FR 82121 (Dec. 29, 2010 and subsequent updates).

available to them, it indicates the response in E-Verify, and the employer will receive the Employment Authorized notification.

If SVO is unable to confirm employment eligibility, E-Verify displays a Tentative Non Confirmation (TNC)[5] response and generates a Further Action Notice (FAN) for the employer to print and give to the employee. The FAN explains why the employee has received a TNC and what steps the employee needs to take before E-Verify can provide an Employment Authorized response. The FAN also explains the employee's rights and provides information about contesting the TNC result. If the employee wishes to contest the TNC, the employee must notify his or her employer, who indicates so in E-Verify. E-Verify will then generate a Referral Date Confirmation notice that provides the employee with the date by which the employee must visit SSA or contact DHS to begin resolving the TNC. If the employee resolves the TNC, E-Verify will provide a final Employment Authorized response to the employer. If the employee cannot resolve the TNC, or the employee chooses not to contest the TNC and the employer indicates to E-Verify that the employee will not contest, E-Verify will generate a Final Non Confirmation (FNC) response for the employer and the employer may choose to terminate the individual's employment or continue to employ the individual. If the employer chooses to continue to employ the individual, the employer must notify DHS of that continued employment.

Reason for the PIA Update

USCIS is updating DHS/USCIS/PIA-030 and its subsequent updates to account for the following enhancements:

1. A new interconnection between E-Verify and NLETS, to collect and verify information related to individuals' driver's licenses, driver's permits, and state-issued identification (ID) cards.

2. The use of the Person Centric Entity Resolution microservice,[6] which is designed to improve accuracy and efficiency of the existing E-Verify automated verification process to determine if the information supplied by the employer matches an identity in existing USCIS, DHS, and external source systems.

3. VIS migrated to a cloud-hosted environment.

[5] A TNC means that the information entered into E-Verify does not match records available to SSA and/or DHS. It is possible for an employee to receive a dual TNC, which means the case received a TNC result from both agencies at the same time because information entered into E-Verify does not match records available to both SSA and DHS. E-Verify identifies the agency or agencies associated with the mismatch in the TNC Further Action Notice.

[6] A microservice is an approach to application development in which a large application is built as a suite of modular services. Each module supports a specific business goal and uses a simple, well-defined interface to communicate with other sets of services.

E-Verify Enhancements

NLETS

E-Verify previously validated MVA information using data from the American Association of Motor Vehicle Administrators (AAMVA) as described in the E-Verify RIDE PIA.[7] E-Verify partnered with ten MVAs via AAMVA to validate driver's license and state ID data entered by employers in E-Verify. The employer entered the issuing state and driver's license or state ID number and if there was a match in the state's MVA database, then AAMVA returned additional driver's license or state ID data to E-Verify.

With the publication of this PIA and revised E-Verify SORN,[8] E-Verify uses an alternative source for validating driver's license and state ID information, and determining the quality of the information, through a different entity called NLETS.[9] NLETS is a computer-based message switching system that links together and supports most state, local, and federal law enforcement, justice, and public safety agencies for the purpose of securely sharing and exchanging critical information. Entities using and sharing information through NLETS include states and territories within the United States, the District of Columbia, federal agencies with a justice component, select international agencies, and a variety of strategic partners that serve the law enforcement community. All of these entities work cooperatively to exchange data through NLETS.

E-Verify only uses NLETS to obtain information related to validating driver's licenses and state IDs from MVAs. An NLETS transaction allows for E-Verify to validate driver's license and state ID information directly from the state MVAs. For example, USCIS does not maintain driver's license data; however, E-Verify needs to validate the driver's license or state ID provided by the employee. The NLETS interconnection allows USCIS to expand fraud prevention measures by allowing access to a larger source of driver's license data (from 10 states[10] under separate AAMVA agreements to nearly all 50 states, as well as the District of Columbia and Puerto Rico, under one single information sharing agreement) to match against and support a growing volume of E-Verify users. NLETS accesses other data, but only the MVA data will be available to E-Verify. The information provided to NLETS from USCIS is the same as what USCIS provided to AAMVA, including name, date of birth, license type, license status, and license number.

When a driver's license or state ID is presented to establish identity, the driver's license or state ID number is entered into E-Verify by the employer. In order to verify the authenticity of the presented information, E-Verify validates the information against NLETS records via the

[7] *See* DHS/USCIS/PIA-030(c) E-Verify RIDE, *available at* www.dhs.gov/privacy.

[8] *See* DHS/USCIS-011 E-Verify Program SORN, 79 FR 46852 (August 11, 2014). A revised DHS/USCIS-011 E-Verify SORN is being published concurrently with this PIA.

[9] NLETS is a private not-for-profit corporation created by the 50 state law enforcement agencies.

[10] These states include Maryland, Wyoming, Arizona, Florida, Iowa, North Dakota, Nebraska, Idaho, Wisconsin, and Mississippi.

Enterprise Service Bus (ESB).[11] E-Verify sends NLETS the driver's license or state ID number and, NLETS will return, the name, address, date of birth, physical description, Social Security number (SSN), driver's license type, restrictions, driver's license or state ID status, and driver's license or ID number to ESB. Since NLETS cannot issue a response tailored for E-Verify's purposes, ESB is configured so that the data elements that are not pertinent to the validation process (i.e., address, physical description, SSN, and restrictions) will not be accessed or stored by E-Verify. The unnecessary data elements will not be sent to the audit logs and will never be made available to USCIS personnel, E-Verify participants, or any USCIS system. Further, for increased security measures, ESB will only send a match or no-match response to E-Verify, which will be displayed to the E-Verify user.

If an NLETS query results in a mismatch, the case will be sent to SVO, which manually validates biographic information against multiple systems, one of which would be NLETS. SVO is responsible for the accurate and efficient handling of E-Verify verification requests. SVO conducts the manual process by querying the individual's name, date of birth, and gender. SVO may query NLETS using the Person Centric Query Service (PCQS).[12]

Person Centric Entity Resolution microservice

USCIS introduced a new Person Centric Entity Resolution microservice as an enhancement to E-Verify. The Person Centric Entity Resolution microservice uses enhanced algorithms to compare employee verification requests against existing USCIS, DHS, and external systems to determine if the information supplied by the employer matches an identity in existing source systems. The former logic was a distributed architecture in which VIS aggregated and compared data from multiple systems for E-Verify. With each employee verification submission, VIS previously queried each system independently, which impacted the source system's availability and operational functionality. In the event the source systems were down, verification requests were sent to SVO to manually validate biographic information against multiple systems.[13]

E-Verify's use of the Person Centric Entity Resolution microservice does not change the overall E-Verify verification process. The Person Centric Entity Resolution microservice supporting E-Verify continues to access the same data from the same systems as VIS. However, the Person Centric Entity Resolution microservice now retrieves that information through a direct connection to Enterprise Citizenship and Immigrations Services Centralized Operational

[11] The ESB services enable the seamless integration, communication, and exchange of data between systems and from different operating systems. *See* DHS/USCIS/PIA-008(a) Enterprise Service Bus, *available at* www.dhs.gov/privacy.

[12] *See* DHS/USCIS/PIA-010 Person Centric Query Service, *available at* www.dhs.gov/privacy.

[13] *See* DHS/USCIS/PIA-030 E-Verify Program to learn more about the manual resolution process and the associated systems used to reconcile TNCs, *available at* www.dhs.gov/privacy.

Repository (eCISCOR)[14] and Customer Profile Management System (CPMS),[15] and facilitates the same external data calls via Enterprise Service Bus (ESB).[16] The Person Centric Entity Resolution microservice retrieves, consolidates, and caches data from the following systems on a daily basis:

USCIS Systems

- eCISCOR
  - Computer-Linked Application Management Information System (CLAIMS 3)[17]
  - Computer-Linked Application information Management System (CLAIMS 4)[18]
  - Reengineered Naturalization Application Casework System (RNACS)[19]
  - Marriage Fraud Amendment System (MFAS)[20]
  - Global (not an acronym)[21]
  - Central Index System (CIS)[22]
  - RAILS (not an acronym)[23]
- CPMS

DHS Systems via ESB

U.S. Customs and Border Protection (CBP)

- Arrival and Departure Information System (ADIS)[24]
- CBP TECS (not an acronym) system[25]

[14] *See* DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* www.dhs.gov/privacy.
[15] *See* DHS/USCIS/PIA-060 Customer Profile Management Service (CPMS), *available at* www.dhs.gov/privacy.
[16] *See* DHS/USCIS/PIA-008(a) Enterprise Service Bus, *available at* www.dhs.gov/privacy.
[17] *See* DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* www.dhs.gov/privacy.
[18] USCIS is preparing to decommission CLAIMS 4 in its entirety. All forms formerly processed in CLAIMS 4 will be processed in USCIS ELIS. For more information on USCIS ELIS, *see* DHS/USCIS/PIA-056(a) USCIS Electronic Immigration System (USCIS ELIS), *available at* www.dhs.gov/privacy.
[19] RNACS decommissioned data is available in eCISCOR. *See* DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* www.dhs.gov/privacy.
[20] MFAS decommissioned data is available in eCISCOR. *See* DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* www.dhs.gov/privacy.
[21] Global is replacing the Refugees, Asylum, and Parole System. *See* DHS/USCIS/PIA-027(c) USCIS Asylum Division, *available at* www.dhs.gov/privacy.
[22] *See* DHS/USCIS/PIA-009(a) Central Index System (CIS), *available at* www.dhs.gov/privacy.
[23] RAILS has replaced the National File Tracking System. RAILS is only used for assistance in linking consolidated A-Numbers and links between A-Numbers and Receipt numbers. No biographic information is contained in this system, and no data from RAILS is directly passed to E-Verify users or to VIS. RAILS can be used by USCIS employees to find the A-Files. *See* DHS/USCIS/PIA-075 RAILS, *available at* www.dhs.gov/privacy.
[24] *See* DHS/CBP/PIA-016(a) I-94 Website Application, *available at* www.dhs.gov/privacy and DHS/CBP/PIA-024 Arrival and Departure Information System, *available at* www.dhs.gov/privacy.
[25] *See* DHS/CBP/PIA-021 TECS System: Platform, *available at* www.dhs.gov/privacy.

U.S. Immigration Customs and Enforcement (ICE)

- Student and Exchange Visitor Identification System (SEVIS)[26]
- ENFORCE Integrated Database (EID) Enforcement Alien Removal, Module (EARM)[27]

External Sources via ESB

- Department of State (DOS) Consular Consolidated Database (CCD) Passport[28]
- Department of Justice (DOJ) Executive Office Immigration Review (EOIR) [29]
- American Association of Motor Vehicle Administrators (AAMVA)[30]
- National Law Enforcement Telecommunications System (NLETS)[31]

This enhanced effort associates information from multiple USCIS, DHS, and external sources within one location. Under the enhanced verification process, when E-Verify verifies an individual's employment eligibility, VIS communicates with the Person Centric Entity Resolution microservice to instantaneously access the same data from all systems as opposed to checking each system one by one for a match. The Person Centric Entity Resolution microservice then applies algorithms to determine a match confidence level, which is a measurement of the level of confidence in the match between the information submitted by the employer and the information received from the data source. The Person Centric Entity Resolution microservice algorithms enable the resolution and aggregation of multiple un-linked identity records (and associated data) to form a singular, comprehensive, and high-confidence view of an individual; thus, making the employment eligibility verification matching process more reliable.

Additionally, because the Person Centric Entity Resolution microservice caches[32] all the necessary data, E-Verify has a reduced dependency on other systems' availability. E-Verify's use of the Person Centric Entity Resolution microservice has significantly improved E-Verify reliability and speed by accessing the same data from all USCIS, DHS, and external systems

[26] *See* DHS/ICE/PIA-001 Student Exchange Visitor Information System (SEVIS), *available at* www.dhs.gov/privacy.

[27] *See* DHS/ICE/PIA-015(b) ENFORCE Alien Removal Module (EARM 3.0), *available at* www.dhs.gov/privacy.

[28] ESB does not access CCD directly, but does so through an existing interface with CBP's TECS. *See* Consular Consolidated Database (CCD) Version 04.00.00, *available at* https://www.state.gov/documents/organization/242316.pdf.

[29] *See* DOJ Case Access System for EOIR, *available at* https://www.justice.gov/sites/default/files/opcl/docs/eoir_pia.pdf.

[30] AAMVA operates AAMVAnet. However, the data in the system is owned by the organization that had the original authority to collect the data.

[31] NLETS owns the database, but the information comes directly from the States' DMV databases.

[32] Note that "caching" does not introduce a new lag in the data because the data are being replicated in real-time from the same sources, or VIS is receiving the data faster because nightly (24 hour delayed refresh) processes are eliminated by direct interfaces: for instance, Card and Card Photo information in legacy requires a nightly ingestion method on 24 hour stale data from CPMS via ESB, whereas we now have a live replication of data directly from CPMS.

instantaneously (as the systems can be queried by the Person Centric Entity Resolution microservice at the same time) as opposed to checking each system one by one for a match. E-Verify makes a more precise search since the Person Centric Entity Resolution microservice associates the data it has queried from USCIS, DHS, and external source systems in a way to make the employment eligibility verification matching process more accurate.

The Person Centric Entity Resolution microservice improves how E-Verify confirms employment eligibility by reconciling data in a new, highly optimized manner. Instead of VIS relying on individual systems for each employment verification submission case, VIS interfaces with the Person Centric Entity Resolution microservice as a single source to provide access to the same data sets for the automated verification process. This results in reduced response times and a reduction of the number of TNCs; and therefore, a reduction in the number of manual verifications. By leveraging this improved data, E-Verify is able to deliver more accurate results to customers in a quicker fashion.

Migration to Cloud-based Platform

USCIS is undergoing a system modernization effort.[33] To support this modernization effort, USCIS is shifting away from traditional Data Centers to the use of third-party cloud-hosted environments. USCIS migrated VIS to the Amazon Web Services (AWS) cloud platform. This migration does not impact the collection and use of personally identifiable information (PII) in VIS. USCIS requires AWS to segregate VIS data from all other third-party data. All existing records from VIS were extracted from the legacy database and transferred to the new cloud environment. This technological advancement does not impact the collection and use of records in VIS, but modifies the way USCIS stores and maintains E-Verify records.

Privacy Impact Analysis

Authorities and Other Requirements

The legal authority to operate E-Verify does not change with this update. USCIS continues to cover this collection of information by IIRIRA,[34] which required DHS to establish a Basic Pilot Program with voluntary participation by employers who could use a system to determine whether newly hired employees are authorized to work in the United States. This program was subsequently renamed E-Verify. Specifically, Section 404(d) requires that the system be designed and operated to maximize its reliability and ease of use, and with appropriate administrative, technical, and physical safeguards to prevent unauthorized disclosure of personal information, enabling DHS to offer enhanced services to improve the reliability of the records used by E-Verify for work authorization.[35] The authority provided by IIRIRA extends to these enhancements to E-Verify, as

[33] USCIS is undergoing a system modernization effort to align with the Cloud Smart initiative. Cloud Smart is a new strategy for agencies to adopt cloud solutions that streamline transformation and embrace modern capabilities.
[34] IIRIRA §§ 401-05, 8 U.S.C. § 1324a note.
[35] IIRIRA § 404(d), 8 U.S.C. § 1324a note.

both enhancements improve accuracy and efficiency of the automated verification process while reducing the potential use of fraudulent information for employment eligibility verification.

USCIS has a member agreement and a contract in place with NLETS regarding the terms, conditions, safeguards, and procedures in place in order to exchange information.

The E-Verify Program SORN,[36] continues to cover the collection, maintenance, and use of the information for the enhanced automated employment verification process. A revised version of the SORN is being published concurrently with this PIA to add a new Routine Use that covers disclosing information to NLETS. The forthcoming revised SORN will allow for routine access to MVA information via NLETS. The collection of information associated with the Person Centric Entity Resolution microservice is still compatible with the purpose of the E-Verify SORN because the collection and use of information better and more reliably permits E-Verify to confirm an individual's eligibility for employment in the United States. No new information is being collected or used as a result of E-Verify's use of the Person Centric Entity Resolution microservice as part of the automated verification process.

This update does not change the Authority to Operate (ATO) for VIS, the technology that supports E-Verify. VIS was approved for operation on April 28, 2014, and is part of the Ongoing Authorization program. Ongoing Authorization requires VIS to be reviewed on a monthly basis to ensure compliance with security and privacy requirements in order to maintain its ATO.

The records schedule does not change with this update. Data will be retained for 10 years after the final match determination in accordance with NARA approved records retention and disposal schedule N1-566-08-07.

This update does not impact the Paperwork Reduction Act (PRA) requirements for the E-Verify Program. Collection of information for the E-Verify Program is covered by the Paperwork Reduction Act, specifically, by OMB Control number 1615-0092 (E-Verify Program); and OMB Control number. 1615-0047 (Form I-9, *Employment Eligibility Verification*).

Characterization of the Information

This update does not impact the data elements collected for E-Verify. The same information will continue to be used to conduct employment eligibility queries; however, NLETS will be used to access driver's license and state ID data, and data will be accessed differently through the use of the Person Centric Entity Resolution microservice.

NLETS

USCIS accesses MVA driver's license and ID data through NLETS. The NLETS enhancement will collect the same data elements AAMVA previously did in order to validate driver's licenses and state ID information. The data element used is the driver's license or state ID

[36] See DHS/USCIS-011 E-Verify Program SORN, 79 FR 46852 (August 11, 2014). A revised DHS/USCIS-011 E-Verify SORN is being published concurrently with this PIA.

number, but if that comes back with no record, NLETS is queried again using the name, date of birth, and gender to determine if there is a possible mismatch.

The source of the information is still the MVA databases. However, instead of having access to driver's license and state ID information for only 10 MVAs through AAMVA, NLETS allows USCIS access to driver's license information for nearly all 50 states, the District of Columbia and Puerto Rico. This increases USCIS' ability to verify a larger percentage of driver's licenses and state IDs as well as improves the reliability of the employment eligibility verification process.

Privacy Risk: There is a risk that the NLETS data may be inaccurate.

Mitigation: This risk is not mitigated. USCIS is not responsible for the accuracy of the MVA driver's license data in NLETS. The MVAs are the source of the data and they maintain and update the data in NLETS.

Privacy Risk: There is a risk of an over collection of information and that NLETS will share data elements that are not associated with the employment verification process with USCIS.

Mitigation: This risk is mitigated. USCIS sends NLETS the driver's license or state ID number and, in return, USCIS will receive the name, address, date of birth, physical description, SSN, driver's license type, restrictions, driver's license or state ID status, and driver's license or state ID number. In order to confirm the driver's license or state ID information given to USCIS by the employee, USCIS only requires the name, date of birth, driver's license type, driver's license or state ID status, and driver's license or state ID number from NLETS. However, NLETS does not have a tailored response configuration for USCIS so the data elements that are not pertinent to the verification process (address, physical description, SSN, and restrictions) are not stored by USCIS. The address, physical description, SSN, and restrictions will not be sent to the audit logs and will never be made available to USCIS personnel, E-Verify participants, or USCIS systems. Further, for increased security measures, the ESB will strip all data fields and only send a match or no-match response to E-Verify (which is displayed to the E-Verify user).

Person Centric Entity Resolution microservice

E-Verify's use of the Person Centric Entity Resolution microservice does not impact the collection of information or the sources of information for E-Verify. The Person Centric Entity Resolution microservice accesses the same data from the same systems as E-Verify currently does in order to verify employment eligibility, but through a live feed from eCISCOR, a direct connection to CPMS, and through ESB. The Person Centric Entity Resolution microservice retrieves data from various USCIS source systems and then associates the data from those systems. In addition, it queries the same external systems that VIS did. This data is then used by E-Verify instead of E-Verify relying on data in its nightly feeds or having to go out to different systems.

The Person Centric Entity Resolution microservice retrieves and caches information from the source systems in near real-time. The Person Centric Entity Resolution microservice correlates multiple records belonging to one individual by using a strong matching algorithm that includes matching, for example, A-Number along with other biographic identifiers to determine a match confidence score. A match confidence score is a measurement of the level of confidence in the match between the information submitted by the employer and the information received from the data source. Submissions that do not meet the match confidence threshold are routed to the E-Verify manual resolution process.

USCIS SVO identifies inconsistencies between databases as part of the E-Verify manual resolution process. SVO searches other data sources to produce definitive results. Once SVO has resolved the problem, they update E-Verify to reflect an Employment Authorized result for the employee. If SVO cannot resolve the problem they will update E-Verify to issue a Final Nonconfirmation.

Privacy Risk: There is a risk that information retrieved via eCISCOR, ESB, and CPMS, as opposed to directly, may be inaccurate, which may adversely affect the final determination.

Mitigation: USCIS mitigates this risk by getting data via real time interfaces from systems like ADIS, CLAIMS 4, RNACS, TECS, and SEVIS. In addition, some systems send nightly batches to VIS. This enables VIS to have updated and current data increasing the reliability of the employment eligibility verification process.

Uses of the Information

There are no new uses of this information resulting from the enhancements to E-Verify. USCIS continues to use E-Verify to provide an automated process to compare information provided by an employee on Form I-9, *Employment Eligibility Verification*, which the employer enters into E-Verify, against information in DHS, DOJ, DOS, and state MVA databases to confirm employment eligibility as outlined in the E-Verify PIA[37] and SORN.[38] The enhancements bring greater accuracy and efficiency to the employment eligibility verification process by allowing USCIS to verify driver's license and state ID information against nearly all 50 state MVAs, and comparing that information against existing USCIS, DHS, and external systems to determine if the information supplied by the employer matches an identity in existing source systems.

Notice

USCIS is providing general notice about the E-Verify enhancements through this PIA update. USCIS is also concurrently issuing a revised E-Verify SORN[39] to cover the direct connection to NLETS to verify driver's license and state ID information. In addition, the Privacy Notice located on the instructions for Form I-9, *Employment Eligibility Verification*, notifies

[37] *See* DHS/USCIS/PIA-030 E-Verify Program, *available at* www.dhs.gov/privacy.
[38] *See* DHS/USCIS-011 E-Verify Program SORN, 79 FR 46852 (August 11, 2014). A revised DHS/USCIS-011 E-Verify SORN is being published concurrently with this PIA.
[39] *See* DHS/USCIS-011 E-Verify Program SORN, 79 FR 46852 (August 11, 2014). A revised DHS/USCIS-011 E-Verify SORN is being published concurrently with this PIA.

individuals of USCIS' authority to collect information, and the purposes, routine uses, and consequences of declining to provide the information to USCIS. Therefore, through the E-Verify verification process, individuals are provided notice of the use of their information for employment eligibility verification purposes, including the sources that USCIS uses. Lastly, the myE-Verify and E-Verify.gov websites provide additional information about verification processes and individual E-Verify case history.[40]

Privacy Risk: There is a privacy risk that individuals providing information to USCIS do not receive sufficient notice that explains their information is being stored on a server not owned or controlled by USCIS.

Mitigation: This risk is partially mitigated. This PIA update provides notice that information is stored in a cloud-based system, and USCIS provides general notice to individuals about the collection and use of their information. USCIS, however, does not provide explicit notice at the time of collection that the information may be stored in a cloud-based system. Regardless of storage location of records, VIS records are governed by USCIS' collection, use, and dissemination of personally identifiable information and are required to meet all applicable federal security guidelines.

Data Retention by the project

This update does not impact the retention of information in E-Verify. Data will be retained for 10 years after the final match determination in accordance with NARA approved records retention and disposal schedule N1-566-08-07.

Information Sharing

NLETS

With this update, USCIS connects to NLETS in order to query the state MVA databases for the purpose of verifying driver's license and state ID information. USCIS is sharing and receiving data to and from NLETS. In cases in which there is a mismatch and require manual verification, SVO would query by driver's license or state ID number or name/date of birth/gender. SVO would query NLETS via PCQS. This is the same process as outlined in the E-Verify RIDE PIA.[41] No other information from Form I-9 will be shared with NLETS.

Person Centric Entity Resolution microservice

E-Verify's use of the Person Centric Entity Resolution microservice does not impact existing external sharing arrangements as described in the E-Verify Program PIAs. The Person Centric Entity Resolution microservice retrieves, consolidates, and caches data from most of the external source systems through the ESB in support of the automated verification process (except for SSA's Numident). The previous process required VIS, through the ESB, to send and retrieve

[40] Please see https://www.e-verify.gov/about-e-verify/commitment-to-privacy for more information.

[41] *See* DHS/USCIS/PIA-030(c) E-Verify RIDE, *available at* www.dhs.gov/privacy.

the individual's biographic information from external source systems with each employment eligibility verification request. This enhanced process no longer requires VIS to send individual requests to external source systems (except for SSA's Numident, which VIS continues to query). The Person Centric Entity Resolution microservice retrieves and stores batched data from USCIS systems (via the ESB) on a daily basis to serve as the single, back-end repository. In addition, the Person Centric Entity Resolution microservice queries the external systems that VIS directly queried before except for SSA's Numident, which VIS continues to query.

Migration to Cloud-based Platform

USCIS migrated VIS to the AWS cloud platform. This migration does not impact information sharing practices in VIS from the previous legacy system. USCIS requires AWS to segregate VIS data from all other third-party data. The cloud-hosted VIS system absorbed legacy VIS functionality and system interconnections.

Redress

This update does not impact how access, redress, and correction may be sought through USCIS. There are two ways to correct incorrect information. Inaccuracies identified during the E-Verify process will result in an employee receiving a TNC. Employees 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.

USCIS also continues to provide individuals with access to their information through a Privacy Act or Freedom of Information Act (FOIA) request. Individuals not covered by the Privacy Act or Judicial Redress Act (JRA) still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. U.S. citizens and Lawful Permanent Residents may also file a Privacy Act request to access their information. If an individual would like to file a Privacy Act or FOIA request to view his or her USCIS records, the request can be mailed to the following address:

National Records Center
Freedom of Information Act/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

Persons not covered by the Privacy Act or JRA are not able to amend their records through FOIA. Should a non-U.S. person find inaccurate information in his or her records received through FOIA, he or she may visit a local USCIS Field Office to identify and amend inaccurate records with evidence.

Auditing and Accountability

USCIS ensures that practices stated in this PIA comply with federal, DHS, and USCIS standards, policies, and procedures, including standard operating procedures, rules of behavior, and auditing and accountability procedures. VIS is maintained in the AWS, which is a public cloud designed to meet a wide range of security and privacy requirements (e.g., administrative, operational, and technical controls) that are used by USCIS to protect data in accordance with federal security guidelines.[42] AWS is Federal Risk and Authorization Management Program (FedRAMP)-approved and authorized to host PII.[43] FedRAMP is a U.S. government-wide program that delivers a standard approach to the security assessment, authorization, and continuous monitoring for cloud services.

USCIS requires VIS to undergo the security assessment process to verify adherence to DHS privacy and security requirements. USCIS validates technical and security controls to preserve the confidentiality, integrity, and availability of the data during the security authorization process. These technical and security controls limit access to USCIS users and mitigates privacy risks associated with unauthorized access and disclosure to non-USCIS users. Further, DHS security specifications require auditing capabilities that log the activity of each user in order to reduce the possibility of misuse and inappropriate dissemination of information. All user actions are tracked via audit logs to identify information by user identification, network terminal identification, date, time, and data accessed. All USCIS systems employ auditing measures and technical safeguards to prevent the misuse of data.

All USCIS employees with access to E-Verify receive annual mandatory privacy awareness and Information Security training. These trainings present Privacy Act responsibilities and policies regarding security, sharing, and safeguarding of official information and PII on USCIS systems. The trainings are updated as appropriate, and all USCIS employees are required to take these trainings annually.

Privacy Risk: The data maintained by AWS for the purposes of cloud hosting may be vulnerable to breach because security controls may not meet system security levels required by DHS.

Mitigation: This risk is mitigated. USCIS is responsible for all PII associated with the VIS system, whether on a USCIS infrastructure or on a vendor's infrastructure, and it therefore imposes strict requirements on vendors for safeguarding PII data. This includes adherence to the DHS 4300A Sensitive Systems Handbook, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program.[44]

Privacy Risk: There is a risk that E-Verify records can be accessed by unauthorized personnel since VIS resides in AWS, a public cloud.

Mitigation: This risk is mitigated. Although VIS operates in a public cloud, VIS is separated from other public cloud customers. VIS operates in a Virtual Private Cloud, which is a

[42] Public clouds are owned and operated by third-party service providers whereas private clouds are those that are built exclusively for an individual enterprise.
[43] https://marketplace.fedramp.gov/#/product/aws-us-eastwest?status=Compliant&sort=productName.
[44] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

private component to the public cloud. USCIS controls access to the systems within the cloud, not AWS.

Responsible Official

Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security