Privacy Impact Assessment Update
for the

E-Verify Mobile App Usability Testing

DHS/USCIS/PIA-030(f)

January 15, 2016

<u>Contact Point</u>
Donald K. Hawkins
Privacy Officer
United States Citizenship Immigration Services
(202) 272-8030

<u>Reviewing Official</u>
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), United States Citizenship and Immigration Services (USCIS) has developed an E-Verify mobile application ("the App") to support users who wish to access E-Verify using a mobile device. USCIS will initially perform usability testing for the App with users from a select group of enrolled employers. USCIS is conducting this Privacy Impact Assessment (PIA) because during the usability testing period, USCIS will collect Personally Identifiable Information (PII) through the App as part of the existing employment eligibility verification process. No PII will be stored on the mobile device. If E-Verify expands usage of the App or changes its functionality beyond current E-Verify functionality, this PIA will be updated.

Introduction

E-Verify is a voluntary[1] Internet-based system that allows enrolled employers to confirm the employment eligibility of their employees to work in the United States. E-Verify employers electronically verify the employment eligibility of newly hired employees by matching information provided by employees on Form I-9 Employment Eligibility Verification (Form I-9) against existing information contained in the Verification Information System (VIS).[2] E-Verify was mandated by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA).[3]

Traditionally, an employer's centralized human resource (HR) representative manually processes Form I-9 in hard copy or on a desktop computer. The information from the completed Form I-9 is then manually entered into E-Verify via a desktop computer or submitted via Web Services.[4]

As mobile technology has evolved, employers are now incorporating a wider array of devices, including tablets and smart phones, to support remote hiring and mobile HR processing. To better support these employers, USCIS has been working to expand and improve options to use E-Verify across mobile platforms and devices.

[1] Although E-Verify remains voluntary, some employers may be required to use E-Verify as a condition of contracting, as the result of a court order, or by operation of federal or state law.

[2] VIS is a composite information system that checks the data entered by the employer against data from the Department of Homeland Security (DHS), the Social Security Administration (SSA), the U.S. Department of State (DOS), and certain state Department of Motor Vehicle divisions. For information on VIS and the E-Verify process, *see* DHS/USCIS/PIA-030 E-Verify Program PIA, available at www.dhs.gov/privacy.

[3] The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law (P.L.) 104-208, September 30, 1996. E-Verify was originally designated as the "Basic Pilot" program. IIRIRA directs DHS to "maximize [E-Verify's] reliability and ease of use" by persons and other entities making elections. *See* IIRIRA Sec. 404(d)(1).

[4] Web Services describes a method of communicating between electronic devices through the internet.

In 2012, E-Verify became mobile-optimized. This allowed users to access E-Verify using a mobile device's web browser. Users could create and manage cases on their mobile device, but E-Verify did not automatically reformat according to the device's screen size. Users still experienced the layout and function of E-Verify as if on a desktop and were required to repeatedly scroll and adjust the device's screen view to perform basic functions. As a result, mobile use of E-Verify from 2012 to the present has been limited. In 2014 the U.S. Senate Appropriations Committee issued a Report[5] to the 2014 DHS Appropriations Bill (Report). The Report directed USCIS to develop an E-Verify mobile application and other smartphone technologies to encourage small business use of E-Verify.[6] The App provides a flexible, effective, easy to use tool that can be adapted to a variety of business models, including small businesses. It encourages use of E-Verify and supports employer compliance with the legal requirement to employ only individuals who may legally work in the United States and USCIS's mission to ensure the integrity of the U.S. immigration system.

The App usability testing phase includes the design, development, and limited deployment of a free, native[7] application that provides enrolled users a new way to access E-Verify to create and manage E-Verify cases. The App is a significant step to meeting the directive of the Senate Appropriations Committee report and allows E-Verify to better support employers who have shifted from a traditional HR back-office hiring process to a mobile hiring process.

Users can download the free App to their device from the Apple App Store. Once installed, users can access the App on their device and log in using their existing E-Verify credentials. Individuals who do not have an E-Verify account are required to access E-Verify from a web browser on their mobile device or a computer to enroll in E-Verify and complete the required tutorials before using the App.

Information sent to or received by the App is transmitted using Hyper Text Transfer Protocols with Secure Socket Layers ("https") which encrypt and protect the information in transit. The mobile device must have and maintain an active Internet connection to use E-Verify. If the Internet connection is unavailable, the user will not be able to access E-Verify via the App. If the Internet connection is lost, the user will be required to recreate the E-Verify case. If the user leaves the E-Verify App to use another application, the user will lose the connection to the App and will be required to login again. Information collected through the App is not retained on

[5] U.S. Senate Committee on Appropriations, Report to Accompany H.R. 2217; S.Rpt. 113-77, July 18, 2013. Available from www.gpo.gov (http://www.gpo.gov/fdsys/pkg/CRPT-113srpt77/pdf/CRPT-113srpt77.pdf).

[6] Small businesses provide 55% of all jobs and have provided 66% of all net new jobs since the 1970s. In addition, since 1990, as big business eliminated 4 million jobs, small businesses added 8 million new jobs. *See* U.S. Small Business Administration. *Small Business Trends: Small Business, Big Impact!* Retrieved from: https://www.sba.gov/content/small-business-trends-impact.

[7] A native application is an application program that has been developed and coded for use on a particular platform or device. It is installed through an application store and appears as an icon on a device's home screen.

the mobile device at any time.

For the initial usability testing phase, when a user opens the App, a link to the Privacy Act Statement will appear at the bottom of the login page. If the App is approved for a national launch, the Privacy Act Statement will appear as a pop-up screen when the user is asked to enter information. Users may click the link to review the full Privacy Act Statement and the statement will also be available in the Apple App Store and Apple TestFlight.[8]

Once users log in to the App, they may begin creating and processing verification cases using information from an employee's Form I-9 as they would do if accessing E-Verify from a web browser. The App has been designed to function and provide users with case results in the same manner as if the user were accessing E-Verify from a web browser. In addition, the App will use the device's camera to capture images of employee documents when required as part of a verification query. The App contains code which allows captured images (e.g. the front and back of an Employment Authorization Card) to be temporarily held[9] on the device and to be re-sized and stitched into a single image before it is submitted to DHS.[10] The original and resized images captured by the camera in the App are not permanently stored on the user's device, but are transmitted directly to DHS. The App does not have access to the device photo album and the App does not allow the user to save the captured images to the device. If the user leaves the App, before submitting the image, the image will be lost. The user will have to log back in to the App and repeat the image capture and submission process.

This App's wireless print capability relies on a third-party library that contains code used to monitor the device's GPS receiver. The information enables the device to identify available printers and wireless printing services across device platforms. DHS does not receive or retain a user's location information as a result of using the App.

Users can voluntarily self-report actual performance time through the Apple TestFlight feedback tool as part of usability testing. Screens look different (e.g., data fields will be stacked instead of laid-out horizontally) as the experience will be customized for mobile devices, but the information collected to run E-Verify cases is the same.

USCIS is developing the App using an iterative approach. The initial product contains

[8] Apple TestFlight is a beta testing site which allows an App to be tested by a limited group of users before an App is added to the Apple App Store. Only those users who have volunteered to participate in usability testing are provided with the email link for TestFlight.

[9] Images are deleted from the users' device once submitted to DHS. The original and resized images captured by the camera in the App are not permanently stored on the user's device, but are transmitted directly to DHS. The App does not have access to the device photo album and the App does not allow the user to save the captured images to the device.

[10] In the current desktop process as well as the app, when an employee presents his or her employer an Employment Authorization Document (EAD) or Permanent Resident Card, the employer will review onscreen the DHS held photo associated the EAD or Permanent Resident Card. If the employer indicates the photos do not match, the employer submits a copy of the document to DHS for further review.

basic functionality that allows previously registered E-Verify users to log-in and create and manage cases. It also serves as the technical foundation for USCIS to build future enhancements if additional iterations of the App are funded. If funded, App updates will be made available in the Apple App Store. Users will be notified through their devices and directed to make updates when an update is available.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given the particular technologies and the scope and nature of their use, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of the E-Verify Mobile Application operations as it relates to the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

In accordance with the Paperwork Reduction Act (PRA) of 1995,[11] USCIS publishes an information collection notice in the Federal Register to obtain public comments regarding the

[11] The usability testing phase covered by this PIA is a limited usability test of the App. USCIS will publish information about the App in accordance with the Paperwork Reduction Act (PRA) when the decision is made to

nature of the information collection, the categories of respondents, the estimated burden (*i.e.*, the time, effort, and resources used by the respondents to respond), the estimated cost to the respondent, and the actual information collection instruments for E-Verify.[12] USCIS also publishes and seeks public comments regarding the collection, storage and use of PII via E-Verify Privacy Act system of records notices in accordance with the Privacy Act of 1974.[13]

The App is an E-Verify enhancement under the terms of the E-Verify Memorandum of Understanding (MOU).[14] Only users who have registered with E-Verify through the E-Verify website will be able to use the App. Users who access E-Verify through the App must abide by the E-Verify MOU requirements.[15] The MOU requires participating employers to clearly display a notice (poster) advising employees that the employer is enrolled in and uses E-Verify. If an employer has difficulty posting E-Verify participation notices because of unique business needs, the employer should ensure that all prospective employees receive the posters with their application materials and that the posters are displayed in a location where potential and current employees are most likely to view them. These posters, which are available in multiple languages, include the statement: “This employer will provide the Social Security Administration (SSA) and, if necessary, the Department of Homeland Security (DHS), with information from each new employee’s Form I-9 to confirm work authorization.” Current Form I-9 instructions clearly advise employees that if they are hired by an E-Verify employer they will be required to provide their Social Security number.

E-Verify also provides public outreach through a website, employer and employee information sessions, and public advertising. E-Verify makes a concerted effort through all its communication to advise employers and employees that USCIS 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.

Privacy Risk: There is a risk that individuals may not have adequate or meaningful notice that DHS has developed and will be testing the App which collects and transmits PII to E-Verify for the purpose of verifying identity and employment eligibility.

Mitigation: This risk is partially mitigated. This PIA provides notice to the individual regarding the App usability testing phase and how the App may be used. The App advises users of the App’s privacy and security features by presenting the Privacy and Security Policy (Policy)

launch the App nationally.

[12] For the latest E-Verify PRA notice, see *Agency Information Collection Activities: E-Verify Program; Revision of a Currently Approved Collection*, 80 FR 32408 (June 8, 2015).

[13] *See* DHS/USCIS-011 E-Verify Program, 79 FR 46852 (Aug. 11, 2014).

[14] *See* http://www.uscis.gov/e-verify/publications/memos/publications-memorandums for samples of the E-Verify MOUs.

[15] *See* the E-Verify Memoranda of Understanding (Revision Date 06/01/13), Article V.2, Modification and Termination.

before the App collects any PII. The Policy clearly articulates the App's compliance with the FIPPs.

The App has a Privacy Act Statement; however, for the initial usability testing phase, a link to the Privacy Act Statement will appear at the bottom of the login page. If the App is approved for a national launch, the Privacy Act Statement must appear as a pop-up screen when the user is asked to enter information. This risk is partially mitigated since users may click the link to review the full Privacy Act Statement and the statement will also be available in the Apple App Store and Apple TestFlight.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress use of PII.

For most employers, participation in E-Verify is voluntary. Federal contractors with contracts containing the Federal Acquisition Regulation (FAR) E-Verify clause[16] and employers in some states are required to use E-Verify either as a condition of contracting or of business licensing. All employers that use E-Verify, whether voluntarily or as the result of a specific mandate must comply with E-Verify requirements, including the protection of PII. Employers may not selectively verify employees or discriminate using E-Verify.

USCIS is performing usability testing for the App by inviting a limited group of currently enrolled E-Verify employers and their registered users[17] to use the App to create and manage E-Verify cases. Users must have completed[18] the E-Verify tutorial on the E-Verify website and associated knowledge test in order to use the App. The usability testing phase will last for 90 days. If a user voluntarily accepts USCIS's invitation to participate in usability testing, the user will receive an email with a link to access Apple TestFlight and download the App.

Once the user downloads the App and completes the required tutorial, the user may login using his or her existing E-Verify credentials and begin creating and managing E-Verify cases using the App. The user will follow the same case creation and case management processes as they would if using the E-Verify web browser. The user must abide by all E-Verify requirements

[16] See 48 C.F.R. § 52.222-54.

[17] Registered users are individuals authorized to create cases on behalf of an E-Verify enrolled employer. Employers register users, then E-Verify assigns the user a user name and password. Users must then complete the E-Verify tutorial before accessing E-Verify. VIS restricts log-in when the user has not completed all required training.

[18] Users who fail to complete a required tutorial will not be able to access E-Verify. A user must view the tutorial and receive a score of 70% or better on the E-Verify knowledge test at the end of the tutorial.

when using the App.

The one difference that a user may encounter when using the App involves cases that result in a data mismatch, or "Tentative Non-Confirmation (TNC)". This will require the employee being verified contact the appropriate federal agency (DHS or SSA) to resolve the data mismatch. Users must print the TNC Further Action Notice and Referral Date Confirmation and provide the employee with copies of the documents. These documents provide information and instructions to the employee on what steps the employee must take to try and resolve the TNC.[19] If the user's mobile device is not print-enabled, the user is required to use the App "Save and Exit" function to save the case information to VIS. The user can then use the "View Cases" or "Search Cases" functions to resume the E-Verify case on a print-enabled device or computer and resume case processing.

If an employee receives a TNC, the employee may contest the TNC result. The procedures for contesting are outlined on the E-Verify website,[20] in the E-Verify User Manual, and in the Further Action Notice. After resolving a DHS TNC, the employee may choose to correct their immigration records. USCIS provides instructions for correcting Form I-551, Permanent Resident Card; Form I-766, Employment Authorization Document; Form I-94; and student or exchange visitor applications on the E-Verify website. Employees may also contact USCIS Customer Support to report employer misuse, privacy violations, and general E-Verify program complaints, through E-Verify Employee Hotline at 1-888-897-7781 or by emailing E-Verify@dhs.gov.

If an E-Verify case results in a final nonconfirmation (FNC), and either the employee or the employer believes the FNC was issued in error, the employer or employee may contact E-Verify to request further review of the case. If E-Verify determines, after review, that the employee is employment authorized, the employer will be provided with updated information in the form of a letter indicating the employee is employment authorized.

Privacy Risk: Individual employees are unable to consent to or control the collection and use of their information through the App if their employer is enrolled in E-Verify and has elected to participate in usability testing.

Mitigation: Although the employee may not consent, he or she is protected in using the App, to the same extent they would be if using the E-Verify web browser. The user must abide by all E-Verify requirements when using the App. E-Verify Customer Support is available to assist employees with questions or concerns.

[19] For a full explanation of the TNC process see DHS/USCIS/PIA-030 E-Verify Program PIA, *available at* www.dhs.gov/privacy.
[20] http://www.uscis.gov/e-verify/employees/how-correct-tentative-nonconfirmation.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

The IIRIRA required DHS 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. Section 404(d) of IIRIRA requires that E-Verify 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. In addition to the requirements of IIRIRA, USCIS developed the App in response to the U.S. Senate Committee on Appropriations directive to develop an E-Verify mobile application and other smartphone technologies to encourage small business use of E-Verify.

The App provides E-Verify users with a new method to access E-Verify and create and manage cases from a mobile device. The App is designed to support employers who are using Internet-enabled technology to shift traditional HR processes to a mobile hiring process and to meet the Senate Committee directive to USCIS to develop a mobile application. Usability testing is the final stage in the design, development, and limited deployment of a free, native Apple App.

There is no privacy risk to purpose specification, as the E-Verify App is consistent with the statutory requirements of IIIRA.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The following information may be used to verify employment eligibility through the App:

- Name (last, first, middle initial, maiden);
- Document Numbers (e.g. A-Number, Visa Number, I-94 Number);
- Social Security number;
- Date of birth;

- Date of hire; and
- Claimed citizenship status.

In the event of a Photo Mismatch TNC, images of the employee documents provided for Form I-9 (e.g., the front and back of an Employment Authorization Card) may be temporarily captured using a registered user's mobile device camera. Images captured by the camera are captured through the App and are not stored on the user's device, but are transmitted directly to DHS.

The App will collect this information in accordance with established E-Verify information collection, retention and destruction requirements. The App will time-out after 15 minutes of inactivity. The mobile device on which the App is used must have and maintain an active Internet connection to use E-Verify. If the Internet connection is unavailable, the user will not be able to access E-Verify via the App. If the Internet connection is lost and a case has not been saved in VIS, the user will be required to recreate the E-Verify case. Information collected through the App is not retained on the mobile device. The App users will be able to retrieve and review case information, including saved cases, from VIS using the App's "View Cases" or "Search Cases" functions.

E-Verify collects and uses the minimum amount of data required to confirm an individual's identity and employment authorization. The App does not use geolocation or cookies to collect information about the employee or user, other than to identify available printers and enable wireless print services. It returns only a minimum of information in response to queries. The information collected is used solely for determining employment eligibility, and is only duplicated or shared when necessary to verify employment eligibility or for specific law enforcement purposes.

The DHS/USCIS-011 E-Verify SORN[21] describes the manner in which DHS will collect, maintain, and disseminate individuals' E-Verify records. In accordance with the NARA retention schedule N1-566-08-7, E-Verify will retain information, including information submitted through the App, 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.[22]

[21] DHS/USCIS-011 E-Verify Program, 79 FR 46852 (Aug. 11, 2014).

[22] See 18 U.S.C. § 3291, the statute of limitations for false statements or misuse regarding passports, citizenship or naturalization documents

Privacy Risk: There is a risk of over-collection of information, specifically location information, needed for the wireless print function of the App.

Mitigation: This risk is partially mitigated. Following the usability test phase, USCIS must include a pop-up consent form that requires the users to consent to the App's use of GPS or location information to locate a printer. USCIS must also determine whether the use of the GPS or location information can be narrowed or reduced in the future.

Employers must have the ability to print a TNC to give it to the affected employee. The printing function within the App is designed to provide a mobile tool for employers who do not have a traditional brick and mortar business model or hiring process that relies on static, hardwired desktop computers. Whether an employee is printing from a local network or via a wireless connected printer, in all cases the user must establish a connection to the appropriate printer and control access to the printed document. Failure to control the document would be considered a potential privacy incident which the employer should report to E-Verify.

This App's wireless print capability relies on a third-party library that contains code used to monitor the device's GPS receiver. The information enables the device to identify available printers and wireless printing services across device platforms. DHS does not receive or retain a user's location information as a result of using the App; however, the App must have a pop-up form that notifies the users that the App will now access their GPS receiver.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

E-Verify may use the information collected through the App to improve and enhance E-Verify's operation and capabilities; to ensure compliance with the E-Verify Program; and to provide customer support and outreach. Please refer to the E-Verify Memorandum of Understanding for Employers (MOU) and E-Verify SORN.[23]

Privacy Risk: There is a privacy risk that information submitted to USCIS via the App could be accessed inappropriately via the wireless submission process.

Mitigation: Employers use the App to submit an employee's Form I-9 information to E-Verify. The App functions in the same manner as the E-Verify web browser. Certain employee information from Form I-9, including name and Social Security number, is compared against

[23] DHS/USCIS-011 E-Verify Program, 79 FR 46852 (Aug. 11, 2014).

Federal Government databases to confirm that the employee is authorized to work in the United States.

Information sent to or received by the App is communicated to VIS using https. Https changes the information sent to or received by the App so it can be read only by the sender and the intended recipient. The information submitted to E-Verify via the App is collected and used in the same manner as information submitted through the E-Verify web browser and follows the same industry and government standard security requirements for receiving sensitive information. The information may be used to prevent fraud and misuse of E-Verify, employment discrimination and document abuse, and employment-based identity theft. On a case-by-case basis, E-Verify may provide law enforcement agencies extracts of information, including information submitted through the App, which identifies potential fraud, discrimination or other illegal activities. USCIS will use existing sharing policies and procedures to ensure that appropriate protections are used when transmitting this information.

Privacy Risk: Insufficient training, monitoring, and accountability controls may result in unauthorized access, disclosure or use of PII

Mitigation: Internal USCIS users of E-Verify take mandatory, annual DHS Information Technology security and privacy awareness training. Internal users are required to complete any testing required by the training program and receive a certificate of completion indicating all training requirements have been met.

External users of E-Verify are provided an on-line tutorial that includes privacy and security training for E-Verify. Users are required to achieve a score of 70% or better when completing the E-Verify tutorial in order to begin creating cases in E-Verify.

Internal and external use of E-Verify and the disposition of all PII is closely monitored to identify and address any breaches or instances of misuse, abuse, or fraud. If a PII breach or misuse is indicated, E-Verify will report such activity as required by law and DHS privacy policies. E-Verify enrolled employers and registered users are required by the terms of the E-Verify MOU to immediately notify DHS in the event of a breach of personal information.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Employers and their employees are responsible for completing Form I-9 and employers who are enrolled in E-Verify must ensure that Form I-9 information submitted to E-Verify via the App is accurate. USCIS provides helper text within the App as well as online resources to support proper completion and data entry. Prior to a submitting a case, users may navigate through information entry screens and to update fields if errors are identified. This provides users with an opportunity to review case information with the employee prior to submitting. In addition, once a case is submitted, if the information entered does not immediately match SSA or DHS records, users are asked to confirm that the information was entered correctly. The user may either confirm that the information matches Form I-9 or change the information in certain fields if the information was entered incorrectly.

Once a case is submitted, E-Verify will provide either an Employment Authorized result or return a TNC indicating the information entered into E-Verify does not match the information in the SSA or DHS databases. If E-Verify results in a TNC, the employer must notify the employee of the TNC and the employee has the option to contest the TNC and contact either SSA or DHS as appropriate to resolve the problem. If the employee provided an email address on Form I-9 and the employer entered it into the E-Verify system, the employee will also receive notice of the TNC result through an email from E-Verify.

If an E-Verify case results in a final nonconfirmation (FNC) for an employee and either the employee or the employer believes the FNC was issued in error, the employer or employee may contact E-Verify to request further review of the case.

Privacy Risk: Inaccurate or incomplete PII data may prevent timely and accurate verification of an individual’s employment authorization and prevent the individual from securing or remaining in employment.

Mitigation: E-Verify users are responsible for ensuring that Form I-9 information submitted to E-Verify via the App is accurate. USCIS provides helper text within the App as well as online resources to support proper completion and data entry. Prior to a submitting a case, users may review information entry screens and to update identified errors. Once a case is submitted, if the information entered does not immediately match SSA or DHS records, users are asked to confirm that the information was entered correctly. If the employee receives a TNC, he or she has eight working days to contest the TNC and resolve any problems.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Using a mobile application to submit sensitive PII to USCIS is a new technical approach to meet the needs of E-Verify’s expanding customer base and to comply with the Congressional directive to develop a mobile application and other smartphone technologies to encourage small business use of E-Verify. This new technology necessarily presents new security challenges.

Privacy Risk: There is a risk that information submitted to USCIS via the mobile application will not be transmitted securely and that the App will not be able to comply with existing technical, operational, and physical security controls as required for typical information technology systems.

Mitigation: E-Verify has implemented a broad range of technical, operational, and physical security measures to protect the App and its information. All E-Verify users are required to register and provide their user name and a strong password to access E-Verify via the App. The App requires users to change their passwords at a specified interval. User accounts are locked after three failed attempts to log on. The App protects against password re-use, and passwords are required to meet length and other specific requirements, e.g., including a special character. Inactive App sessions will time-out, requiring the user to log in again. If the user switches to another application on the mobile device, the App will log off. The user will be required to log in again and, if appropriate, restart the case that was in process when the App closed. Other examples of security controls include:

- Password data is encrypted within the App;
- The App 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 mobile device and VIS;
- VIS passwords are encrypted when making database connections; and
- Procedures are in place to ensure that any potential breaches of information are reported within one hour of being found.

The App does not store any E-Verify information on the device and abides by all existing E-Verify security policies. Users cannot auto-save their passwords in the App. The App is hosted in Apple TestFlight, which is limited access component of the Apple App Store. Information sent to or received by the App is communicated to VIS using https. Https changes the information sent to or received by the App so it can be read only by the sender and the intended recipient. VIS is a secure system which exists within the DHS firewall.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

E-Verify has a comprehensive audit trail tracking and maintenance function that stores information submitted via the App in an audit log that identifies the user who created a case, when the case was processed, the case response, the user who received 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. They are periodically reviewed and used to monitor user activity and compliance with E-Verify requirements. Users of the App are required to comply with all security requirements as outlined in the E-Verify MOU. Attempts to evade the security controls can result in the user's loss of access to E-Verify or termination of the employer's E-Verify account.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in E-Verify may be disclosed outside DHS, except as limited by statute, under a routine use pursuant to 5 U.S.C. 552a(b)(3). Any disclosure of information must be made consistent with the official duties of the person making the disclosure. DHS does not disclose information to consumer reporting agencies.[24]

DHS maintains an accounting of disclosures in the same manner that it maintains all disclosures for E-Verify. The Verification Division (Monitoring and Compliance (M&C)) maintains a log of all case detail extract requests and corresponding disclosures.

There is no privacy risk to the auditing and accountability features in the E-Verify mobile App.

Conclusion

To effectively serve its expanding customer base and to comply with the Congressional directive to develop a mobile application and other smartphone technologies to encourage small business use of E-Verify, DHS has developed a mobile application for E-Verify. The App will allow users to create and process E-Verify cases from a mobile device.

Prior to deployment, DHS will engage in usability testing to validate the App's performance and functionality and to ensure that PII is properly protected and used, a Privacy

[24] See DHS/USCIS-011 E-Verify Program, 79 FR 46852 (Aug. 11, 2014).

Act Statement is posted at initial log-on as a pop-up notice, and that users are notified when the App uses the device’s GPS receiver to locate a printer.

Responsible Officials

Donald K. Hawkins
Privacy Officer
United States Citizenship and Immigration Service

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security