Privacy Impact Assessment
for

myE-Verify

DHS/USCIS/PIA-030(e)

September 12, 2014

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

Reviewing Official
Karen 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) is launching a new service that builds upon E-Verify Self Check called myE-Verify. myE-Verify is a voluntary service that enables individuals access to features that provide greater insight and control into the handling of their personally identifiable information (PII) in E-Verify and Self Check. These features, which USCIS intends to roll out incrementally, include 1) Self Lock, 2) Case History, 3) Case Tracker, and 4) Document Expiration Reminders. USCIS is conducting this Privacy Impact Assessment (PIA) because establishing myE-Verify accounts and accessing its features require individuals to provide PII.

Overview

Background

E-Verify is an Internet-based system that allows enrolled employers to confirm the 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 the Form I-9, Employment Eligibility Verification (Form I-9), against existing information contained in the Verification Information System (VIS), 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.[1] Although E-Verify use 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.

In March 2011, USCIS launched E-Verify Self Check, a free service that enables an individual to check his or her own work authorization status prior to employment and facilitate correction of potential errors in federal databases that provide inputs into the E-Verify process. Through the E-Verify Self Check secure web portal,[2] an individual may check his or her work authorization status by first providing information to authenticate his or her identity, and subsequently providing work authorization information based on information and documents normally provided during the Form I-9 employment eligibility verification process. Prior to E-Verify Self Check, only employers could verify work authorization for employees. With E-Verify Self Check, upon successful identity authentication, an individual may query E-Verify directly.

[1] For information on the E-Verify process, see DHS/USCIS/PIA-030 E-Verify Program PIA, *available at* www.dhs.gov/privacy.
[2] To perform a Self Check, visit http://www.uscis.gov/self-checkUI. For detailed information on Self Check privacy practices, see DHS/USCIS/PIA-030(b) E-Verify Self Check PIA, *available at* http://www.dhs.gov/privacy.

myE-Verify Features and Process

USCIS is launching a new service that builds upon E-Verify Self Check, called myE-Verify, which provides the public greater transparency into the E-Verify system by enabling individuals, through a secure account, access to features that provide greater insight and control into the use of their PII in E-Verify and Self Check. These features, which USCIS intends to release incrementally, include 1) Self Lock, 2) Case History, 3) Case Tracker, and 4) Document Expiration Reminders. The first release of myE-Verify includes account registration and the Self Lock feature. Case History, Case Tracker, and Document Expiration Reminder features will be included in subsequent releases.

Individuals who successfully perform an E-Verify Self Check employment eligibility query and receive an Employment Authorized response can create a myE-Verify account and access all of its features,[3] described below (Note: ***** indicates a feature that USCIS intends to include in subsequent system releases).

- *Self Lock* - is designed to enable an individual to prevent the misuse of his or her Social Security number (SSN) in E-Verify and Self Check. Through a myE-Verify account, an individual can lock his or her SSN from use in E-Verify and Self Check. Any E-Verify queries made by an employer or by an individual via the Self Check service subsequent to placing the lock triggers a DHS Tentative Nonconfirmation (TNC)/DHS mismatch.[4] This means that if an unauthorized individual attempts to fraudulently use a SSN for employment authorization, he or she cannot use the SSN in E-Verify, even if the SSN is that of an employment authorized individual. If the true owner of the SSN receives a DHS TNC (e.g., forgets to unlock his or her SSN through the myE-Verify account before an employer performs an E-Verify query) the individual may contact a DHS Status Verifier to resolve the TNC by providing a document for review (per the standard DHS TNC process) and answering the security questions he or she established when setting up a myE-Verify account.

  To use Self Lock, an individual must log into his or her myE-Verify account and provide his or her SSN and date of birth. This process activates the lock for up to one year (extensions may be made through the account). E-Verify maintains a record of Self Lock transactions (lock and unlock) along with name, SSN, date of birth, email address, security questions and answers, and transaction date. myE-Verify will also send email reminders to account holders at the email address provided during registration to remind them of an impending lock

[3] In a future release that includes Case Tracker, an individual that uses Self Check and receives a response other than "employment authorization confirmed" will be able to create a myE-Verify account; however that individual will not have access to all account features (e.g., Self Lock) until the mismatch is resolved.
[4] For additional information about the E-Verify process and possible outcomes of an E-Verify query such as a tentative nonconfirmation, see DHS/USCIS/PIA-030(d) E-Verify Program PIA, *available at* http://www.dhs.gov/privacy.

expiration.

- *Case History**** – provides greater transparency to individuals about when and how their information was used in E-Verify and Self Check. When logged into a myE-Verify account, a user may generate a report by supplying his or her SSN and DOB. The E-Verify system will be queried in real-time and return a report consisting of the following data elements about each time the individual's SSN was used in E-Verify or Self Check:
    - *Date of use*
    - *Case type (i.e., E-Verify or Self Check)*
    - *Company name*
    - *State*
    - *Result*
    - *Case Verification Number*

  MyE-Verify does not maintain a record of the case history report; a real-time query of E-Verify will generate a report that includes all of the instances in which an account holder's SSN was used in E-Verify and Self Check.
- *Case Tracker**** – provides a mechanism for individuals to track the status of an E-Verify or Self Check case. An individual supplies his or her E-Verify or Self Check case verification number and myE-Verify provides the individual with the status of his or her case and, depending on the status, information about how to move forward with the case. E-Verify does not maintain a transaction of use of Case Tracker; like Case History, myE-Verify uses the case verification number provided to query E-Verify and present the user with the status.
- *Document Expiration Reminders**** – provides email notifications to the account holder before employment authorization documents expire. Document Expiration Reminders do not collect document identification numbers (only document type and expiration date), or check against any other government databases. It is a self-service feature that allows an individual to track expirations in a logical place. Document Expiration Reminder sends emails based on the expiration dates the user provides.

Account Registration and Identity Proofing

Individuals that successfully perform an E-Verify Self Check employment eligibility query and receive an Employment Authorized response may create a myE-Verify account and access all of its features.[5] Individuals who opt to create an account will be prompted to enter

[5] Individuals who do not receive an Employment Authorized response during Self Check will not be able to create an account. A future release will allow for creation of a limited access account (e.g., access to Case Tracker) even if

contact information including email address and phone number; create a username and password; select security questions and responses; and verify two-factor passcode delivery methods (i.e., text, voice, or email address). MyE-Verify will use the email address supplied during registration to send the account holder periodic service announcements and administrative messages related to the account and account features and to send the two factor authentication passcode (if email selected as the option).

Because use of myE-Verify allows access to sensitive data and features beyond employment eligibility status information (e.g., Self Lock), USCIS requires two-factor authentication and an additional identity proofing quiz at a high level of assurance before individuals may access myE-Verify account features.

USCIS uses a separate third-party private sector identity provider (IdP) to establish and maintain myE-Verify accounts. As part of the account registration process, the individual is presented with a quiz containing questions that only he or she should be able to answer. The IdP generates questions based on commercial identity verification information collected by third-party companies from financial institutions and other services providers (e.g., utility and telephone data). USCIS does not have access to or maintain the commercial information. If the IdP cannot generate a quiz or if the user cannot answer the questions, he or she will not be able to set up an account.

In order to generate the quiz, some of the data the user supplied during Self Check (i.e., name, date of birth, and SSN) will be passed to the IdP. To ensure the individual is the same person who originally passed Self Check, these data elements cannot be altered. USCIS does not have access to the quiz questions or the answers provided. USCIS receives a response from the IdP containing the result of the authentication and does not receive or store the individual's plain text SSN or date of birth as part of the myE-Verify account.[6] This is why a user may need to supply his or her SSN or date of birth again to subsequently use some myE-Verify account features, such as Self Lock and Case History. If the user successfully passes identity proofing, he or she must log in using the username, password, and the one-time passcode.

The IdP maintains a record of myE-Verify accounts on behalf of USCIS, including data needed to establish and maintain the account and identity of the person affiliated with the account. DHS also maintains a local database, separate from E-Verify, consisting of information held by the IdP (first name, username, email address (to be used in emails sent by DHS to the

---

he or she receives a mismatch response from Self Check. If the individual wants to use all of the myE-Verify features (e.g., Self Lock, Case History), he or she will have to follow the mismatch process to resolve the mismatch to achieve and Employment Authorized response from Self Check.

[6] DHS stores a hash of the SSN and date of birth the user supplied during Self Check in a local database, separate from E-Verify. The hash of the SSN and date of birth are used to validate the user's SSN and date of birth when the user attempts to establish a lock on his or her SSN or run a Case History report.

myE-Verify account holder), an IdP unique identifier (which ties the user's account to the data held by the IdP)), and a hash ID consisting of the SSN and date of birth the user supplied during Self Check (to be used to validate the user's SSN and date of birth when the user attempts to establish a lock on his or her SSN or run a Case History report). The information contained in this local database does not include the commercial identity verification information the IdP uses to generate the quiz. For Self Lock transactions, USCIS maintains a record in E-Verify including name, SSN, date of birth, email address, security questions and answers provided by the account holder, and transaction date.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA)[7] 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 the E-Verify program. 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.[8] The authority provided by IIRIRA extends to the E-Verify Self Check and myE-Verify, which are enhancements to the E-Verify Program that empower individuals to learn about the use of (e.g., Case History) and exercise limited control (e.g., Self Lock) regarding the use of their information in E-Verify.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

A myE-Verify account enables users access to features associated with data about them covered by the E-Verify Program SORN.[9] The PII associated with the establishment and maintenance of a myE-Verify account is covered by the E-Authentication SORN.[10]

[7] IIRIRA §§ 401-05, 8 U.S.C. § 1324a note.
[8] IIRIRA § 404(d), 8 U.S.C. § 1324a note.
[9] DHS/USCIS-011 E-Verify Program, 79 FR 46852 (Aug. 11, 2014).
[10] DHS/ALL-037 E-Authentication System of Records, 79 FR 46857 (Aug. 11, 2014).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. USCIS completed system security plans (SSP) and the Security Authorization Process in August 2014.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. DHS maintains a transaction record for the use of the Self Lock myE-Verify account feature (SSN, date of birth, user-generated security questions and answers, date and time of the lock) for 10 years in accordance with NARA retention schedule N1-566-08-7, consistent with E-Verify and Self Check queries. myE-Verify accounts are maintained in accordance the NIST *Electronic Authentication Guideline* for seven years and six months beyond the expiration or revocation (whichever is later).[11]

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

This information is covered by the Paperwork Reduction Act and Office of Management and Budget (OMB Control Number 1615-0117 approved on July 24, 2014).

Section 2.0 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.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The project collects information necessary to 1) register and maintain myE-Verify accounts and 2) to facilitate authorized access and use of myE-Verify account features such as Self Lock.

myE-Verify Account Data

Individuals who opt to create an account will be prompted to: enter contact information including email address and phone number; create a username and password; provide self-generated security questions and responses; and verify two-factor passcode delivery methods (text message, voice, or email address). The email address supplied during registration is used to

[11] NAT'L INST. OF STANDARDS &TECH., SP 800-63-2, ELECTRONIC AUTHENTICATION GUIDELINE (2013).

send the account holder periodic service announcements and administrative messages via email related to the account and account features and to send the two factor authentication passcode (if email selected as the option). Please refer to the overview for details on myE-Verify account registration and identity proofing.

myE-Verify Account Features

The following table identifies the information a user will need to supply to use myE-Verify account features:

myE-Verify Feature	**Data collected and used**	**Maintained?**
Self Lock	SSN, DOB	Yes. Self Lock transaction data are maintained in E-Verify including userID, SSN, DOB, date and time of lock or unlock, user-generated security questions and answers.
Case History	SSN, DOB	No. Use of Case History produces a real-time report of SSN use in E-Verify and Self Check
Case Tracker	Case Verification Number	No. Use of Case tracker generates a real-time query in E-Verify and Self Check.
Document Expiration Reminders	Document Type and Expiration Date	Yes. This information is maintained as part of the myE-Verify account data maintained by the IdP.

Additionally, in order to facilitate myE-Verify account holder access to features that rely on work authorization information held in E-Verify, DHS maintains a local database, separate from E-Verify, that includes information held by the IdP (first name, username, email address (to be used in emails sent by USCIS to the myE-Verify account holder), an IdP unique identifier (which ties the user's account to the data held by the IdP)), and a hash ID consisting of the SSN and date of birth the user supplied during Self Check. The hash ID is used to validate the user's SSN and date of birth when the user attempts to establish a lock on his or her SSN or generate a Case History report.

2.2 What are the sources of the information and how is the information collected for the project?

Sources of information for myE-Verify include: 1) the self-reported data entered directly by individuals that successfully complete an E-Verify Self Check query and opt to establish a

myE-Verify account, 2) the E-Verify Self Check service (which passes name, date of birth, and SSN to the IdP and a hash ID based on the SSN and date of birth to USCIS), 3) the third-party private sector IdP for myE-Verify account registration, including identity proofing and account management, and 4) information accessed for the E-Verify basic query.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes, as detailed in Section 2.1, DHS uses a third-party IdP to register and maintain myE-Verify accounts on its behalf; this includes identity proofing. The IdP uses commercial data to perform identity proofing in accordance with the level of assurance guidelines established by the NIST *Electronic Authentication Guideline*.[12] The IdP generates a quiz based on commercial identity verification information, collected by third-party companies from financial institutions, public records, and other service providers. USCIS does not have access to or maintain the commercial identity information, quiz questions, or answers.

2.4 Discuss how accuracy of the data is ensured.

myE-Verify builds on the E-Verify Self Check purpose to facilitate the identification and correction of potential errors in federal databases that provide inputs into the E-Verify system. For example, the Case Tracker feature of myE-Verify, which will be available in future releases, enables an individual to track the status of a mismatch from E-Verify or Self Check and assist him or her in the identification and correction of potential errors in federal databases that provide inputs into the E-Verify system.

To ensure accuracy of the information used by myE-Verify, the information the individual provides as the initial data used to create the account is assumed to be accurate. As noted in the Overview, the third-party private sector IdP performs identity authentication at a high level of assurance. USCIS makes no claims that the data obtained and used for identity verification is accurate or complete. Nevertheless, if an individual believes he or she is unable to authenticate his identity due to inaccurate information accessed by the IdP for identity proofing, he or she is advised to check his or her information at the various credit bureaus through a free credit check site.[13]

[12] NAT'L INST. OF STANDARDS &TECH., SP 800-63-2, ELECTRONIC AUTHENTICATION GUIDELINE (2013).
[13] *See* http://www.consumer.ftc.gov/articles/0155-free-credit-reports and http://annualcreditreport.com.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk of unauthorized disclosure myE-Verify account data.

Mitigation: USCIS mitigates this risk by minimizing data collected to establish a myE-Verify account to the minimum necessary and establishing security measures to protect myE-Verify account data. Specifically, the E-Verify system only maintains the necessary information in its records to perform the Self Lock function and to facilitate myE-Verify account holder access to features that rely on work authorization information held in E-Verify.

DHS maintains a local database, separate from E-Verify, that includes information held by the IdP (first name, username, email address (to be used in emails sent by USCIS to the myE-Verify account holder), an IdP unique identifier (which ties the user's account to the data held by the IdP)), and a hash ID consisting of the SSN and date of birth the user supplied during Self Check. The hash ID is used to validate the user's SSN and date of birth when the user attempts to establish a lock on his or her SSN or run a Case History report. The SSN and date of birth are hashed using a NIST-approved encryption algorithm, which protects the data housed in the local database. USCIS mitigates the risk of a data breach of myE-Verify user data held by the IdP by requiring the IdP to notify DHS of any breaches and complete the required DHS Cyber Incident Reporting Form. The IdP also prepared an Incident Response Plan that outlines the process for handling information security incidents.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

myE-Verify, which provides the public greater transparency into the E-Verify system by enabling individuals, through a secure account, access to features that provide greater insight and control into the use of their PII in E-Verify and Self Check. As noted in Section 2.0, myE-Verify collects information to register and maintain myE-Verify accounts and facilitate authorized access and use of myE-Verify account features such as Self Lock.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. The DHS Headquarters Enterprise Services Division Office developed myE-Verify and manages the interface among the third party private sector IdP, E-Verify, and Self Check.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: A primary risk identified with the establishment of myE-Verify accounts is the risk that an unauthorized individual will be able to access or create an account for another individual which could lead to unauthorized use of the account to obtain access to the individual's sensitive work authorization information and the potential ability to place an unauthorized lock on that individual's SSN.

Mitigation: The primary purpose of creating the Self Lock feature is to protect the authorized individual's SSN from fraudulent use in E-Verify and Self Check. To mitigate these risks associated with unauthorized access and use, USCIS requires a high level of identity assurance and two-factor authentication to establish a myE-Verify account.

As part of the account registration business process, an individual must first pass through E-Verify Self Check, which requires passing an identity proofing quiz. Because a myE-Verify account allows access to sensitive data and features such as Self Lock, myE-Verify requires users to successfully complete a second quiz at a higher level of assurance than the quiz required for Self Check. This means that the quiz will be more difficult for the user to answer; and in turn more difficult for an unauthorized individual to answer correctly. Further, use of two-factor authentication presents a higher barrier to an unauthorized user accessing another individual's account since it would require, in addition to knowing the user's password, also having access to the user's selected delivery method for the one-time passcode. Notwithstanding these risk mitigating practices, in the event it is discovered that an individual fraudulently establishes an account, this issue would be escalated to the IdP to disable the unauthorized account and myE-Verify will release the Self Lock (if one were in place).

Privacy Risk: There is a risk that use of a third-party private sector IdP, such as the risk of use of data supplied by users to create myE-Verify accounts for secondary uses of the data and related query results (e.g., Case History report).

Mitigation: USCIS mitigates this risk through a number of different steps including a Service Level Agreement with the IdP and through the Terms of Service. For example, the Terms of Service clearly identifies that PII supplied during the account registration process will be used solely for issuing credentials and providing identity authentications and will be held no longer than is necessary in order to provide myE-Verify account services. Further, the third-party does not have access to sensitive work authorization information held in E-Verify. In

addition, USCIS is using a trusted Credential Service Provider certified by the FICAM Trust Frameworks Solutions Program.[14]

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The myE-Verify project is subject to the Paperwork Reduction Act process, which made the proposed collection of data to establish a myE-Verify account to use features including Self Lock, Case History, Case Tracker, and Document Expiration Reminders available for public review.

Individuals that opt to create a myE-Verify account also receive notice in the form of Terms and Conditions and a Privacy Statement that the individual must accept before moving forward through the myE-Verify account creation process. When the user accesses myE-Verify account features that require supplying additional information (e.g., SSN and date of birth to establish a Self Lock), another Privacy Act Statement will available to the user explaining the authority, purpose, routine uses, and disclosure.

myE-Verify has also established informational pages on the uscis.gov website to provide information about myE-Verify account features and the process for creating an account. In addition, notice is provided through the E-Verify Program SORN,[15] the E-Authentication SORN,[16] and this PIA.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Like E-Verify Self Check, myE-Verify is a voluntary program. A user may choose to create an account and access all, or some of its features. If an individual does not wish to provide the required information, there are opportunities to exit the web site and choose not to participate.

---

[14] For more information on the Trust Framework Provider process and the privacy criteria used to assess identity providers, such as an IdP, see http://www.idmanagement.gov and http://www.idmanagement.gov/sites/default/files/documents/Guidance_for_Assessors.pdf.
[15] DHS/USCIS-011 E-Verify Program, 79 FR 46852 (Aug. 11, 2014).
[16] DHS/ALL-037 E-Authentication System of Records, 79 FR 46857 (Aug. 11, 2014).

Providing SSN information is necessary to conduct identity authentication at the requisite level of assurance and to access certain account features such as Self Lock. Users are advised of the voluntary nature of the provision of information through Privacy Act statements implemented on the website. Providing this information (including SSN) is voluntary; however failure to provide the requested information will prevent the individual from authenticating his or her identity and obtaining a myE-Verify account.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: USCIS is using a third-party private sector IdP to establish and maintain myE-Verify accounts on its behalf at a high level of assurance requiring the user to answer quiz questions that only he or she should be able to answer. Accordingly, there is a risk, that users may make the incorrect assumption that USCIS maintains commercial identity information about them.

Mitigation: USCIS provides notice in multiple forms including this PIA, the E-Authentication SORN, the myE-Verify Terms and Conditions, and Privacy Statement explaining that the quiz is generated through the third-party IdP based on commercial identity verification information that USCIS does not maintain and cannot access. USCIS does not maintain the quiz questions or responses. The user interface for myE-Verify also uses unique branding and color schemes to indicate to the user that he or she is interacting with the IdP.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

USCIS maintains a transaction record for the use of the Self Lock myE-Verify account feature (name, SSN, date of birth, security questions and answers, date and time of the lock, and email address) for 10 years in accordance with NARA retention schedule N1-566-08-7 consistent with how USCIS maintains employer- and individual-run E-Verify queries. USCIS maintains this information to implement the Self Lock feature, which prevents the individual's SSN from use in E-Verify and Self Check. Any E-Verify queries made by an employer or by an individual via the Self Check service subsequent to placing the lock will trigger a DHS Tentative Nonconfirmation (TNC)/DHS mismatch. This means that if an unauthorized individual fraudulently attempts to use a SSN for employment authorization, he or she will not be able to use the SSN, even if the SSN corresponds to an employment authorized individual.

The IdP maintains myE-Verify account registration data on USCIS's behalf in accordance the NIST *Electronic Authentication Guideline* for seven years and six months beyond the expiration or revocation (whichever is later).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that PII will be retained unnecessarily, which could put information at risk of unauthorized use, access, or disclosure.

Mitigation: USCIS mitigates this risk by applying the data minimization principle, among others, to this project. For example, the E-Verify system only maintains what is necessary in its records to perform the Self Lock – myE-Verify accounts are not "enrolled" in E-Verify but rather, maintained separately on behalf of USCIS by the third party private sector IdP.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. USCIS uses a third-party private sector IdP to establish and maintain myE-Verify accounts. As part of the account registration process, the individual will be presented with a quiz containing questions that only he or she should be able to answer. These questions are generated through the IdP based on commercial identity verification information (USCIS does not have access to or maintain the commercial information), collected by third-party companies from financial institutions and other services providers. In order to generate the quiz, some of the data the user supplied during Self Check (i.e., name, date of birth, and SSN) is passed to the IdP. As noted in the myE-Verify Terms of Service, PII supplied during the account registration process is used solely for issuing credentials and providing identity authentications and will be held no longer than is necessary in order to provide myE-Verify account services.

Self Lock transaction data will not be shared outside of DHS except for the E-Verify data sharing requirements detailed under the Basic Pilot statute. This includes sharing work authorization query data with SSA to facilitate the mismatch resolution processes, as well as sharing data for law enforcement purposes as required by IIRIRA to prevent fraud and misuse of the E-Verify system.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The E-Authentication Records SORN routine use "K" authorizes the sharing specifically "to a trusted third-party identity provider under contract with DHS or certified by the Federal Identity Management Credential and Access Management initiative for the purpose of

authenticating an individual seeking a credential with DHS. The information may be included in the individual's credit record as a "soft inquiry" that does not impact the individual's credit score when the identity provider is a credit bureau or uses a credit bureau to conduct identity proofing. The "soft inquiry" is not viewable by third parties."[17]

The statute that authorizes the operation of E-Verify, IIRIRA, requires DHS to share E-Verify information collected during myE-Verify for limited law enforcement purposes for E-Verify system fraud and misuse and with SSA. Sharing information with SSA is compatible with the original collection because IIRIRA, which requires that USCIS determine whether an individual is work authorized, requires that USCIS use SSA data. Sharing with law enforcement is compatible with the IIRIRA requirement that USCIS prevent fraud and misuse of the E-Verify system.

6.3 Does the project place limitations on re-dissemination?

Yes. With respect to the myE-Verify account information, the myE-Verify Terms and Conditions state that PII supplied during the account registration process will be used solely for issuing credentials and providing identity authentications and will be held no longer than is necessary in order to provide myE-Verify account services.

There is only limited re-dissemination for operational and law enforcement purposes under E-Verify and there is no change under the myE-Verify process. Information from myE-Verify will be shared with SSA; however, SSA only uses the information for E-Verify purposes and will not re-disseminate the information. Sharing with SSA is compatible with the original collection because IIRIRA requires that USCIS determine whether an individual is work-authorized.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

myE-Verify facilitates individuals' access to information about themselves in E-Verify and Self Check. Through audit logs of access to accounts maintained by the third party private sector IdP, USCIS can determine when an individual's account has been accessed.

E-Verify maintains a log of the E-Verify records systems limited dissemination to law enforcement and other Government agencies that align with the IIRIRA requirement that USCIS design the system with appropriate administrative, technical, and physical safeguards to prevent unauthorized disclosure of personal information, and to prevent discrimination and other misuse of the E-Verify system. USCIS maintains and monitors a log of extracts to law enforcement and

[17] DHS/ALL-037 E-Authentication System of Records, 79 FR 46857 (Aug. 11, 2014).

other Government agencies to ensure that sharing complies with the Privacy Act and OMB requirements.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the third party private sector IdP may share data supplied by myE-Verify users to create their accounts for secondary, unrelated uses.

Mitigation: As noted in Section 6.2, the DHS-wide E-Authentication SORN restricts sharing data supplied by myE-Verify users to create their accounts to a trusted third-party identity provider under contract with DHS or certified by the Federal Identity Management Credential and Access Management initiative for the purpose of authenticating an individual seeking a credential with DHS. In addition, the Terms of Service clearly identifies that PII supplied during the account registration process will be used solely for issuing credentials and providing identity authentications and will be held no longer than is necessary in order to provide myE-Verify account services.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

myE-Verify is a vehicle that allows individuals limited control and access to their information in E-Verify and Self Check. Thus, myE-Verify serves as a procedure for individuals to access their information.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

E-Verify Self Check facilitates the identification and correction of potential errors in federal databases that provide inputs into the E-Verify system. There may be instances when an individual is unable to authenticate his identity using the IdP. For example, the IdP may not be able to generate knowledge-based questions if sufficient data pertaining to an individual cannot be located, or when the individual has placed a lock on his or her credit file. In addition, an individual may not receive a passing score because the IdP information maintained is incorrect. If someone is unable to authenticate through the IdP but still wants to determine his or her work authorization status prior to hire, USCIS will provide information on how to visit an SSA field office, access Social Security yearly statements, call USCIS, or submit a FOIA/Privacy Act request to access work authorization records. The individual will also be advised to check the information at the various credit bureaus through a free credit check site.

7.3 How does the project notify individuals about the procedures for correcting their information?

As noted in Section 7.1, myE-Verify seeks to facilitate the correction of potential errors in federal databases that provide inputs into the E-Verify System. Thus, E-Verify Self Check serves a mechanism to allow an individual to correct inaccurate or erroneous information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that an individual will be unable to create a myE-Verify account because he or she cannot pass the identity authentication quiz and will be unable to access myE-Verify account features.

Mitigation: This risk is partially mitigated in that there are alternative means to accomplish some of the myE-Verify account features through the FOIA/PA process. Currently, there is no alternative process for an individual to lock his or her SSN outside of a myE-Verify account.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

USCIS contracted with a third-party private sector IdP to perform credential registration and management functions on its behalf. A Service Level Agreement and Terms of Service contain limitations on the use of PII; specifically limiting use by the IdP to registration process will be used solely for issuing credentials and providing identity authentications and will be held no longer than is necessary in order to provide myE-Verify account services. The IdP and myE-Verify system maintain logs of myE-Verify accounts and provide usage statistics on a macro level (e.g., how many people attempt to and are successfully authenticating their identity, and for those that are not, what are the reasons and why they are having problems, use of certain myE-Verify features). In the event of misuse of a myE-Verify account, USCIS can obtain audit logs of access to individual accounts from the third-party private sector IdP and terminate access to accounts, as appropriate.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS/USCIS employees with access to E-Verify receive annual mandatory privacy awareness training. USCIS will not provide myE-Verify users with any specific privacy training.

USCIS will provide directional guidance on how to register a myE-Verify account and use features such as Self Lock, as described in Section 4.0 regarding notice.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Any individual that successfully passes through Self Check and the myE-Verify account registration, including identity proofing will have access to myE-Verify account features. A limited number of USCIS Verification Division employees and DHS Enterprise Services Division Office employees that manage the myE-Verify project have read-only access to the data held in E-Verify and the local database identified in the Overview that consists of some of the myE-Verify account information held by the IdP on USCIS's behalf. The local database does not contain commercial identity verification information the IdP uses to generate the quiz. The IdP has access to myE-Verify account data but does not have access to the information held in E-Verify.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The program manager, USCIS Office of Privacy, and counsel review all information sharing agreements.

Responsible Officials

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.

_____

Karen Neuman
Chief Privacy Officer
Department of Homeland Security