Privacy Impact Assessment Update
for

myE-Verify

DHS/USCIS/PIA-030(h)

January 24, 2020

Contact Point
Donald K. 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), United States Citizenship and Immigration Services (USCIS) offers online services to individuals that provide greater insight and control into the handling of their personally identifiable information (PII) in E-Verify. Those online services are available through myE-Verify. myE-Verify is a free Web-based service that allows individuals to engage with USCIS and participate in the E-Verify process through a unique and secure account. This secure account allows U.S. workers to review their employment eligibility using the online tools and databases employers who participate in E-Verify use. USCIS is requiring that all users create a USCIS online account through myAccount before using certain myE-Verify features, such as Self Check, Self Lock, and Case History. Previously, individuals could use Self Check and Case Tracker without having a myE-Verify account. USCIS is conducting this Privacy Impact Assessment (PIA) to assess the PII used to create and authenticate accounts to access myE-Verify services, as well as demonstrate how USCIS mitigates associated privacy risks.

Overview

E-Verify, authorized by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA),[1] is a web-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 entering into a federal contract or subcontract that contains the Federal Acquisition Regulation E-Verify clause.[2] 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 DHS program administered by the 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*,[3] against records available to the SSA and DHS.

USCIS launched E-Verify Self Check nationwide in February 2012. Self Check is a free service that enables an individual to check his or her own work authorization status prior to

[1] IIRIRA §§ 401-05, codified at 8 U.S.C. § 1324a note.
[2] As of January 15, 2009, the Federal Acquisition Regulation requires certain federal contractors and subcontractors to use E-Verify to confirm employment eligibility for employees under certain contracts and new hires during the period of those contracts. See 48 CFR § 52.222-54.
[3] Form I-9, *Employment Eligibility Verification*, is *available at* https://www.uscis.gov/i-9.

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, an individual could 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 can query E-Verify directly.

USCIS then introduced a new service that built upon E-Verify Self Check, called myE-Verify. While E-Verify is for employers, myE-Verify is designed for workers and job seekers. myE-Verify gives 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 included Self Lock and Case History.[4] Individuals that successfully performed an E-Verify Self Check employment eligibility case were given the option to create a myE-Verify account and access all of myE-Verify's features. However, individuals did not need a myE-Verify account in order to use Self Check.

Users that opted in to creating a myE-Verify account to access myE-Verify's online services had to go through the account creation process. USCIS used a separate third-party private sector identity provider (IdP) to establish and manage all myE-Verify accounts. The IdP maintained a record of myE-Verify accounts on behalf of USCIS, including data needed to establish and manage the account and identity of the person affiliated with the account. USCIS also maintains a database of user account data, including first name, middle initial, last name, email, Universal Unique Identifier (UUID),[5] and a hashed key consisting of the Social Security number (SSN) and date of birth the user supplied during the account setup and identity authentication process.

Reason for the PIA Update

Previously, all myE-Verify accounts were established and managed by a third-party private vendor. USCIS migrated the account management service for myE-Verify from the vendor to myAccount. myAccount is the USCIS public-facing account management tool that provides users a single sign on experience for its public-facing applications through a USCIS online account. Although myAccount provides single sign on access to participating applications, individuals must request access to each application after setting up their USCIS online account through myAccount.

[4] Users could also use Case Tracker, but again, did not need a myE-Verify account to do so.
[5] A UUID is a system-generated numerical identifier.

myE-Verify is responsible for granting or denying access and maintaining a database of the users accessing its services.

To simplify the account creation process, USCIS removed Self Check as the first step in the account creation process, thus eliminating the need for two identity authentication checks (see figures below). The previous myE-Verify account creation process required users to use Self Check first. In order to use Self Check, the user had to authenticate his or her identity. Once the IdP authenticated the identity of the user, the user could receive confirmation of employment authorization and set up a myE-Verify account. The user would have to authenticate his or her identity again in order to set up a myE-Verify account. Once the user's identity was authenticated, the user could access myE-Verify. This process is illustrated by Figure 1 below.

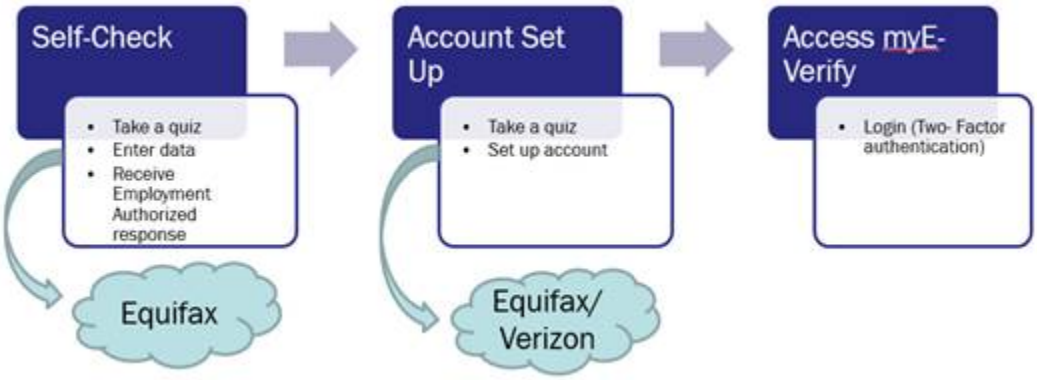

Figure 1. Previous myE-Verify Account Creation Process

With USCIS governing the account creation process instead of relying on a third-party, myE-Verify will now prompt users to create or log in to a USCIS online account through myAccount. Once logged in, users will have access to all the myE-Verify features.

Account Creation

To use any of the myE-Verify online services (with the exception of Case Tracker), individuals must have a USCIS online account. myE-Verify will now leverage myAccount, which is the USCIS enterprise-wide program that manages authentication for USCIS online accounts. USCIS manages myAccount and will be responsible for the establishment and maintenance of all USCIS online accounts.

myAccount provides the public with access to USCIS external-facing systems through a USCIS online account. Users with an existing myE-Verify account under the previous account management vendor are able to sign up for a new account in myAccount to access myE-Verify services. In order to access myE-Verify without any additional identity authentication requirement, the user must: (1) use the same primary email address with both the previous vendor and myAccount, and (2) verify the date of birth and SSN as previously associated with the account.

Individuals who did not previously have a myE-Verify account will need to create an account through myAccount and complete and pass an identity authentication quiz before gaining access to all of the myE-Verify features. This is illustrated by the figure below.

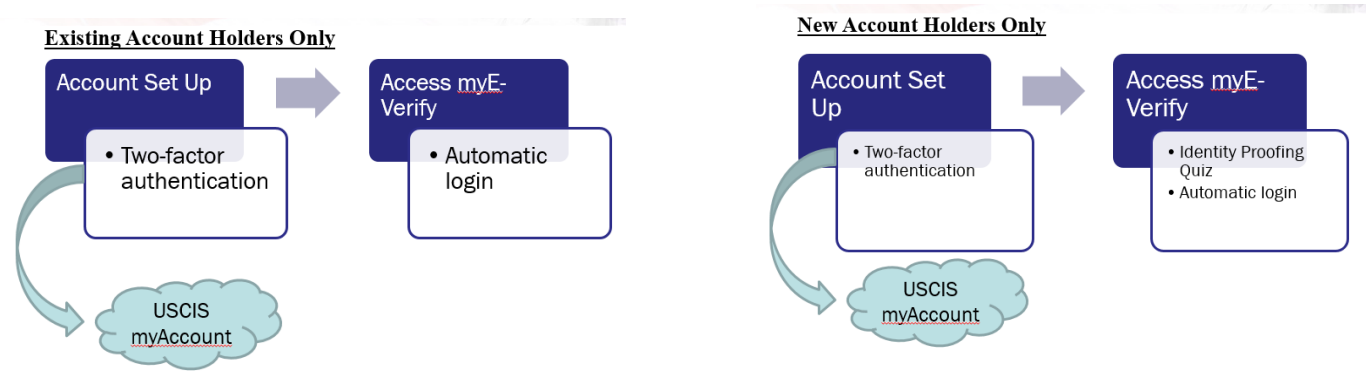

Figure 2. Account Creation Process Using myAccount to Access myE-Verify Services

myAccount allows users to register for a USCIS online account, which then will give the user access to myE-Verify services. In order to register, users who access myE-Verify are redirected to myAccount. To create an account with myAccount, the user first provides an email address. The user verifies possession of the provided email address by clicking a unique link in an email sent to that email address. Then, the user establishes a secure password and a two-step verification method for receiving confirmation codes when logging in, which is detailed in the next section. Once the two-factor authentication is set up and confirmed, myAccount provides the user with an additional Two-Step Verification Backup Code. This code allows users to log in to their account if they lose access to the authentication device (*e.g.*, new mobile device or change mobile numbers). The final step in setting up a myAccount is to select five security questions from a drop down list and provide "fill-in-the-blank" answers. This allows users to use the self-service tool to reset their own password. USCIS does not use the answers to these questions for purposes other than assisting with password resets.

USCIS online account passwords and answers to the security questions are centrally stored within myAccount. Passwords are not visible to USCIS. The answers to the security questions are only visible to USCIS customer help desk personnel who assist with password resets.

Two-Factor Authentication

The USCIS online account is created through myAccount and connects to myE-Verify. myAccount uses a two-step factor authentication method by means of a Short Message Service (SMS), email, or using an authentication application from a mobile device. The two-step factor authentication adds an extra layer of security by requiring users to sign in to their account using two steps: 1) Something you know (such as a password) and 2) Something you have (such as a mobile phone or a security key/code).

myAccount assigns a UUID to each account created. myAccount will pass the UUID and email address to myE-Verify for those users requesting access to myE-Verify. myE-Verify leverages myAccount's authentication services[6] in order to provide high confidence that the user controls the authenticators bound to the USCIS online account, such as email address, mobile phone number, or third-party authenticator application (*e.g.*, Google Authenticator, Authy, Microsoft Authenticator). If the user chooses to use an email address, he or she will receive an email each time he or she signs in. If the user chooses to use a mobile phone number, he or she will receive a text message to the mobile device each time he or she signs in.

The user can use any third-party authenticator application available on the device of his or her choice. The third-party authenticator application generates security codes for signing into sites that require a high level of security. If the user chooses to use a third-party authenticator application, he or she is provided instructions on how to connect to the third-party authenticator application. The selection and use of a third-party authenticator application is at the discretion of the user. USCIS does not prescribe a specific authenticator application. The user will receive a separate USCIS notice recommending that the user reviews the privacy policy of the third-party authenticator application since USCIS has no control over the third-party policies.

To access myE-Verify via myAccount, USCIS requires proof of possession and control of two distinct authentication factors through secure authentication protocols. Each time the user logs in, the user is required to provide myAccount with the email address used for the account, the password, and the two-step verification code. The user credentials are sent to myAccount for verification and authentication.

Identity Authentication using a Third-Party Identity Proofing Service

In order to gain full access to myE-Verify services, USCIS uses a third-party IdP service to generate a quiz containing questions that only the user should be able to answer. These questions are generated by the IdP service based on commercial identity verification information (USCIS does not have access to the commercial information) collected by third-party companies from financial institutions and other service providers.

In order to generate the quiz, myE-Verify will ask the user to provide his or her first name, middle initial, last name, address, date of birth, SSN, and mobile number. All of these data elements are required in order for the IdP to authenticate the user's identity. myE-Verify will pass this information to the IdP. The IdP will then run a check on the data provided and generate questions based on the person's identity and return those questions to myE-Verify. myE-Verify presents the questions to the user, collects the responses, and sends the responses back to the IdP

[6] In this case, authentication is the process or action of verifying electronically that a person is who he or she claims to be. Thus, USCIS must ensure that identity of an account holder that is asserted belongs to the person to whom that account belongs. Credentials that the account holder provides are compared to those on file. If the credentials match, the account holder is granted authorization for access.

for verification. The IdP then returns a pass/fail indicator to myE-Verify. If the user passes the quiz, myE-Verify grants the user full access to all of its features, including Self Check.

Privacy Impact Analysis

Authorities and Other Requirements

The legal authority to administer myE-Verify does not change with this update. IIRIRA[7] 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 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 E-Verify 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.

This PIA update does not change the applicable Systems of Records Notice (SORN). The E-Verify Program SORN continues to cover the collection, maintenance, and use of the information contained within the myE-Verify services.[9] The collection of information associated with myE-Verify is still compatible with the purpose of the E-Verify Program SORN because the collection and use of information permits USCIS to administer its E-Verify program and carry out its responsibilities under IIRIRA. myE-Verify also continues to be covered by the DHS E-Authentication Records System of Records,[10] which covers the information collected to establish and maintain a USCIS online account. No new information is being collected or used as a result of requiring a USCIS online account to access Self Check.

This update does not change the Authority to Operate (ATO) for the Verification Information System (VIS), the underlying technical system 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. DHS maintains a record of the E-Verify query and response to the query conducted via Self Check and a transaction record for the

[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, 84 FR 28326 (June 18, 2019).
[10] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).

use of the Self Lock account feature (*i.e.*, SSN, date of birth, user-generated security questions and answers, date and time of the lock) for 10 years in accordance with the National Archives and Records Administration (NARA) approved records retention and disposal schedule N1-566-08-07.

The IdP will maintain the information collected for identity authentication purposes in accordance with NIST Special Publication (SP) 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing,* 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, and NIST SP 800-63C, *Digital Identity Guidelines: Federation and Assertions* as it is subject to the same guidelines. Certain information from the myE-Verify accounts managed by the previous third-party vendor continue to maintain in accordance with SP 800-63B, . The data that the previous third-party vendor maintains is the UUID. The UUID is associated to identifying information that was already contained within the previous third-party vendor's credit reporting database (*i.e.*, name, SSN, date of birth). These elements are separate from the USCIS data, as the USCIS data was purged in accordance with the contract. The previous third-party vendor is also storing information that was collected to generate the attribute score given to the user during the identity authentication process (*i.e.*, transaction IDs, timestamp of the identity verification, and attribute score values returned).

This PIA update does not impact the Paperwork Reduction Act requirements for myE-Verify. Collection of information for myE-Verify is covered by the Paperwork Reduction Act, specifically, by OMB Control number 1615-0117 (*Form G-1499*, *myE-Verify*).

Characterization of the Information

Users that had a myE-Verify account prior to April 29, 2019, are now required to establish a USCIS online account through myAccount if they wish to continue using the services. Existing users will need to set up their USCIS online account using the same email address they used to create their previous myE-Verify account. If an email address is found in the myE-Verify database, myE-Verify will prompt the user to provide his or her date of birth and SSN to validate that the individual coming in and creating the USCIS online account is the same individual that previously set up the myE-Verify account. Once that information is validated, the user is logged into myE-Verify and can access all of the features.

If an existing user provides a different email address than what he or she used to create his or her previous myE-Verify account, then myAccount will process the user as a new user. The user will be required to go through identity authentication.

Users that did not previously have a myE-Verify account will have to create a myAccount and undergo an identity authentication process. myAccount collects the user's email address, password, password reset questions and answers, and mobile number (if the user selects SMS for two-factor authentication). myAccount will also store that information, in addition to the UUID that is assigned by myAccount but is not shown to the user. Once the user passes the two-factor

authentication process with myAccount, he or she is redirected back to myE-Verify in order to complete the identity authentication process.

myE-Verify collects account management data (*e.g.*, the user's full name, address, SSN, date of birth, mobile number, identity-based quiz answers, email address), challenge questions, and answers for Self Lock, and document information for Self Check.[11] myE-Verify also stores some of the account management data, such as the user's full name, email address, SSN, date of birth, and the UUID passed from myAccount. The SSN and date of birth are stored in a hashed format.

The IdP generates the identity-based quiz questions from information it gets from myE-Verify, such as name, address, SSN, date of birth, mobile number. The IdP uses that identifying information to look up the individual in order to generate the identity-based quiz questions from commercial identity verification information (USCIS does not have access to the commercial information) collected by third-party companies from financial institutions and other service providers. These questions are displayed back to the user through the myE-Verify User Interface. myE-Verify will collect the responses to these questions and submit them back to the IdP. The IdP also uses the mobile number to verify that the mobile number provided in the identity authentication process matches the name on the mobile account, in addition to performing other fraud and risk checks. Providing a mobile number is optional for creating a USCIS online account, but it is required for myE-Verify's identity authentication process. The IdP stores all of the identity attributes passed to its application from myE-Verify and the IdP's response.

VIS stores case-related data, such as the user's name, SSN, date of birth, challenge questions and answers for Self Lock, Self Lock Receipt number, and document information for Self Check.

The figure below documents the entity that collects and stores the data elements that pertain to establishing a USCIS online account, maintaining a USCIS online account, and accessing myE-Verify services.

[11] Document information includes citizenship attestation, documents used for verification (such as passport), document number, document expiration date, and country of issuance (foreign passport), which is data that E-Verify already collects.

	myAccount		myE-Verify		IdP		VIS	
	Collect	Store	Collect	Store	Collect	Store	Collect	Store
First Name			X	X	1	2		X
Middle Initial			X	X	1	2		X
Last Name			X	X	1	2		X
Email	X	X	X	X	1	2		
Password	X	X						
UUID		*		X		*		
Password Reset Challenge Questions	X	X						
Password Reset Challenge Answers	X	X						
Mobile Number	X	X	X		1			
Street Address			X		1	2		
City			X		1	2		
State			X		1	2		
Zip Code			X		1	2		
Social Security Number			X	**	1	2		X
Date of Birth			X	**	1	2		X
Identity-Based Quiz Questions					3	3		
Identity-Based Quiz Answers			X		1	2		
Challenge Questions for Self Lock			X					X
Challenge Answers for Self Lock			X					X
Self Lock Receipt Number								X
Document Information for Self Check			X					X
VIS Case Number								X
VIS Case Result								X

KEY

* UUID is a unique identifier assigned to a user by myAccount and the IdP independently of each other.

** SSN and date of birth are stored in a hashed format.

1: myE-Verify collects the data and passes to the IdP. The IdP stores this data in a transaction log along with the IdP's pass/fail response.

2: The IdP is storing these elements that are associated to the UUID and are already contained within the IdP's credit reporting database. These elements are separate from the USCIS data. The IdP is also storing information that was collected to generate the attribute score given to the user during the identity authentication process (*i.e.*, transaction IDs, timestamp of the identity verification, and attribute score values returned).

3: Identity-Based Quiz Questions are generated by the IdP and passed to myE-Verify to display to the user.

Figure 3: Data Collection and Storage Matrix

Information is also collected through the services that myE-Verify offers. Once logged into myE-Verify, an individual can use Self Check. Self Check allows individuals to check their own employment eligibility by checking information against the databases E-Verify uses when employers enter a case. The information collected from the individual is dependent on his or her citizenship status and his or her document choices. These include: SSN, Citizenship Status; Alien Number; Passport Number; I-94 Number; and/or Permanent Resident or Employment Authorization Document Card Number. This is the same information that is used to determine employment eligibility in the E-Verify work authorization process.

USCIS maintains a record of the individual's E-Verify case including his or her name, date of birth, SSN, work authorization documentation information, the case result, and an E-Verify case number. This is consistent with how E-Verify cases initiated by authorized employers are maintained in E-Verify.

Privacy Risk: In order to use the E-Verify Self Check service, an individual must have a USCIS online account. During account creation, the individual must pass identity authentication. There is a risk that some individuals will not be able to access myE-Verify services because their identity cannot be authenticated (and thus, the individual cannot use the Self Check service at all).

Mitigation: This risk is not mitigated. It is important to note that Self Check is not a required service. In this first step of the service, if an individual does not pass the identity authentication portion, there is no formal process to address the inability to verify identity.[12] There are several reasons why an identity cannot be authenticated. For example, an individual may not have resided in the country long enough to establish a credit or address history and therefore his or her identity could not be verified. Another reason could be that the information contained in the commercial databases is incorrect; thus, there is insufficient accurate information in which to develop questions to authenticate. It is also possible that an individual is attempting to illegitimately access myE-Verify. However, even if the individual fails to pass the identity authentication portion, that does not mean that he or she will not be work authorized through E-Verify. Failure to pass identity authentication will neither deny anyone the ability to seek employment within the United States nor have any repercussions to the individual (such as being terminated from a job). Employers are not notified that the individual did not pass identity authentication. There are still avenues available to the U.S. workforce to check on the accuracy of their SSA and DHS records.[13]

[12] There is no formal process with myE-Verify, but the individual can request a free credit report and address any discrepancies with his or her credit information with the appropriate credit reporting agency.
[13] *See* DHS/USCIS/PIA-030 E-Verify Program, *available at* www.dhs.gov/privacy.

Privacy Risk: There is a risk of collecting account creation information from individuals who are now required to create USCIS online accounts in order to use Self Check (whereas previously, these individuals were not required to create a secure account).

Mitigation: This risk is mitigated. USCIS is requiring Self Check users to create a USCIS online account to enhance the security of the system. USCIS underwent an analysis to determine which data elements were relevant and necessary for the purposes of creating an account and facilitating identity verification. Self Check will require individuals to authenticate their identity through the IdP, and provide a SSN to enhance the ability of the IdP to generate knowledge-based questions.

Privacy Risk: There is a risk that existing myE-Verify accounts may be incorrectly linked to a USCIS online account created through myAccount.

Mitigation: This risk is mitigated. Existing users will need to set up their USCIS online account using the same email address they used to create their previous myE-Verify account. If an email address is found in the myE-Verify database, myE-Verify will prompt the user to provide his or her date of birth and SSN to validate that the individual coming in and creating the USCIS online account is the same individual that previously set up the myE-Verify account. If an existing user provides a different email address than what he or she used to create his or her previous myE-Verify account, then myAccount will process the user as a new user. The user will be required to go through identity authentication.

Privacy Risk: There is a risk that one account created through myAccount could have multiple identities associated with it due to myAccount providing services for other USCIS services.

Mitigation: This risk is not mitigated. myAccount allows users to create multiple accounts with different email addresses; however, myE-Verify can only allow one account per identity (email and SSN). USCIS is developing a solution to prevent this issue.

Uses of the Information

There are no new uses of this information resulting from the changes to the Self Check business process. USCIS continues to use Self Check to provide an automated service to individuals who wish to check their own work authorization status prior to employment and facilitate correction of potential errors in federal databases that provide inputs into the E-Verify process as outlined in the previous E-Verify PIAs.[14] The change allows for a simplified account creation process by eliminating the need for two identity authentication checks. myE-Verify will still offer all the same services (Self Check, Self Lock, and Case History),[15] but a USCIS online account is required in order to access these services.

[14] *See* DHS/USCIS/PIA-030 E-Verify Program, *available at* www.dhs.gov/privacy.
[15] Case Tracker is still a service under myE-Verify, but it does not require an account.

Notice

USCIS is providing general notice about system changes through this PIA update. The individual is also provided a Privacy Notice before he or she begins the account creation process (through myAccount), before he or she begins the identity authentication process, and on the myE-Verify homepage where the various services are accessed. At each step of the process, an individual is given notice of the use, collection, and maintenance of his or her information. Additionally, the myE-Verify website, E-Verify.gov website, and myAccount website provide additional information about the USCIS online account creation process and identity authentication process.[16] Lastly, notice is provided in the myE-Verify Terms of Service, which the individual must accept before moving forward through the identity authentication process.

Privacy Risk: There is a privacy risk that individuals providing information to USCIS do not receive sufficient notice that explains they must now set up a USCIS online account before using Self Check.

Mitigation: This risk is mitigated. This PIA update provides notice that individuals must set up a USCIS online account before using Self Check, and USCIS provides general notice to individuals about the collection and use of their information. The public is also given notice about this change on the myE-Verify website.[17]

Privacy Risk: There is a privacy risk that individuals do not receive sufficient notice that explains how myAccount manages user account data for multiple USCIS services.

Mitigation: This risk is mitigated through the publication of this PIA update, which provides notice that myAccount manages user account data for multiple USCIS services.

Data Retention by the project

This update does not impact the retention of information in E-Verify. DHS will continue to maintain information for 10 years in accordance with NARA-approved records retention and disposal schedule N1-566-08-07. The previous account management vendor will maintain the data[18] collected for identity authentication purposes in accordance with the NIST *Electronic Authentication Guideline* for seven years and six months beyond the expiration or revocation (whichever is later).[19] The current IdP stores information for six months online and 10 years offline based on the NARA approved records retention and disposal schedule N1-566-08-07.

---

[16] Please see https://www.e-verify.gov/about-e-verify/commitment-to-privacy or https://myaccount.uscis.dhs.gov/terms for more information.
[17] *See* https://myeverify.uscis.gov/.
[18] Although the DHS information has been purged from any contractor-owned system(s) that was used to process DHS information, the previous vendor is still required to retain the data for a certain amount of time.
[19] National Institute of Standards and Technology, SP 800-63-2, *Electronic Authentication Guideline* (2013).

Privacy Risk: There is a risk that information will be retained beyond the retention period due to using a third-party IdP for identity authentication services, which could lead to unauthorized access to the information.

Mitigation: This risk is mitigated. The current IdP adheres to the NARA approved records retention and disposal schedule N1-566-08-07. The contract also outlines that the IdP is required to verify when the data is deleted by submitting proof to USCIS.

Privacy Risk: There is a risk that the previous vendor continues to retain information related to USCIS transactions beyond the termination of the contract. There is a risk the vendor will retain data beyond the retention period, which could lead to unauthorized access to the information.

Mitigation: The previous vendor is required to adhere to the *DHS 4300A Sensitive Systems Handbook*, which states that the previous vendor must certify that DHS information has been purged from any contractor-owned system(s) that was used to process DHS information.[20] The previous vendor is also required to adhere to all Federal Identity, Credential, and Access Management (FICAM) requirements, which outline a seven years and six months data retention period from last valid credential expiration or contract termination. After this period, the previous vendor will destroy the data in compliance with the FICAM requirements.

Information Sharing

USCIS will no longer use a third-party vendor to establish and maintain myE-Verify accounts, but will now rely on myAccount to maintain the USCIS online accounts created to access myE-Verify services. USCIS will continue using a third-party IdP to authenticate the identities of individuals as outlined above.

Privacy Risk: There is a risk that the previous vendor will share the information it received from USCIS through the identity authentication process.

Mitigation: This risk is mitigated. The previous vendor is using the information USCIS provided to verify against data it already knows. If the data provided is not already contained in the vendor's database, then the result comes back as a no match. The vendor does not incorporate any USCIS provided data into its database.

Redress

This update does not impact how access, redress, and correction may be sought through USCIS. myE-Verify allows users to directly and securely engage with USCIS to obtain their work authorization information. Users who create an account must authenticate their identity using the user name, password, and authentication code. Once authenticated, individuals may access the information they used to create their myE-Verify profiles, such as the primary email address,

[20] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

recovery email/backup email, password, two step verification method (text, email, authentication application), mobile phone number, password reset questions, and backup code.[21] Users can protect their identities by preventing unauthorized use of their SSN in E-Verify and seeing where and when their information has been used in E-Verify and Self Check.

E-Verify Self Check, a service under myE-Verify, 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 a Social Security Administration field office, access Social Security yearly statements, call USCIS, or submit a Freedom of Information Act/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.

Auditing and Accountability

This update does not impact the auditing and accountability processes. The previous vendor adhered to the *DHS 4300A Sensitive Systems Handbook*, which provides implementation criteria for the rigorous requirements mandated by DHS's Information Security Program, including data removal from contractor-owned system requirements.[22] The previous vendor will certify that it has decommissioned the system it used to support the identity authentication process for USCIS. USCIS will archive the data in accordance with NARA requirements. The previous vendor will also archive the data in accordance with FICAM requirements.

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. USCIS contracted with a third-party IdP to perform identity verification functions on its behalf. A Service Level Agreement and Terms of Service contain limitations on the use of PII. Limiting use by the IdP to providing identity authentication ensures that PII will be held no longer than is necessary in order to provide that service.

To prevent misuse of myE-Verify, users are restricted from submitting an SSN that was not used during the identity authentication step in the account creation process for the purposes of Self Check, obtaining a case history report, or locking/unlocking an SSN. Further, a user cannot change the SSN, date of birth, or name that was used to create the account.

[21] Users can request a new backup code, but they cannot edit the code.
[22] *See* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

MyAccount maintains logs of USCIS online accounts; however, these logs do not specify which services the account uses. The IdP transaction log includes information submitted by the user (*i.e.*, name, address, date of birth, and SSN), whether the user correctly answered the questions, the scores generated during the identity authentication process, and the business rules that were triggered during the transaction. In the event of misuse of a USCIS online account, USCIS can terminate access to accounts at its discretion.

The IdP and myE-Verify system also provide customer 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).

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