Privacy Impact Assessment
for the

E-Verify Self Check

DHS/USCIS/PIA-030(b)

September 06, 2013

Contact Point
Donald K. Hawkins
Privacy Officer
United States 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 United States Citizenship and Immigration Services (USCIS) Verification Division has developed a service called E-Verify Self Check. The E-Verify Self Check service is voluntary and available to any individual who wants to check his own work authorization status prior to employment and facilitate correction of potential errors in federal databases that provide inputs into the E-Verify process. When an individual uses the E-Verify Self Check service he will be notified that either 1) his information matched the information contained in federal databases and would be deemed work-authorized, or 2) his information was not matched to information contained in federal databases which would be considered a "mismatch." If the information was a mismatch, he will be given instructions on where and how to correct his records. USCIS conducted this privacy impact assessment (PIA) because E-Verify Self Check collects and uses personally identifiable information (PII).[1]

Overview

Background

E-Verify was mandated by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104-208, September 30, 1996. Section 404(d) requires that the system be designed and operated to maximize the reliability and ease of use. Therefore, the Department of Homeland Security (DHS) developed E-Verify Self Check.

The E-Verify Program is a free and mostly voluntary DHS program implemented by the USCIS Verification Division and operated in collaboration with the Social Security Administration (SSA) to determine work authorization.[2] It compares information provided by employees on the Employment Eligibility Verification, Form I-9, against information in SSA, DHS, and Department of State (DOS) databases in order to verify an employee's work authorization.

In order to enable an individual to check his own work authorization status prior to employment and facilitate correction of potential errors in federal databases that provide inputs into the E-Verify process, USCIS developed E-Verify Self Check. Through the E-Verify Self Check secure web portal, an individual will be able to check his work authorization status by first providing information to authenticate his identity, and subsequently providing work authorization information based on information normally provided Form I-9 employment documentation. Prior to E-Verify Self Check, only employers could verify work authorization for newly-hired employees. With E-Verify Self Check, upon successful identity authentication an individual may query E-Verify directly. If the information provided by the individual matches the information contained in federal databases (SSA, DHS, DOS) a result of

[1] DHS is updating and making clarifications to the DHS/USCIS/PIA-030(b) published on March 4, 2011, regarding DHS's retention of PII. This PIA replaces the version published on March 4, 2011.

[2] E-Verify is a voluntary program except for employers that operate within a state that has passed legislation mandating the use of E-Verify (e.g., Arizona and Mississippi) or for employers subject to the E-Verify Federal Contractor Final Rule contained in the Federal Acquisition Regulation (FAR). The E-Verify Federal Contractor Rule (FAR 22.18) directs federal agencies to require many federal contractors to use E-Verify to electronically verify the employment eligibility of certain employees.

"work authorization confirmed" is displayed to the individual. If the information was a mismatch, the individual will be provided a result of "Possible mismatch with SSA" or, "Possible mismatch with Immigration Information." E-Verify Self Check will also provide the individual with instructions on how to facilitate correction of these potential errors in records contained in these federal databases should the individual choose to do so prior to any formal, employer run E-Verify query process.[3] In rare cases, an individual may still receive a potential mismatch during a normal E-Verify query because the record cannot be changed. The individual is not required to correct the record mismatches that were identified by E-Verify Self Check.

E-Verify Self Check Process

E-Verify Self Check service involves a two-step process: 1) identity authentication of the individual; and 2) an E-Verify query to confirm the individual's current work authorization status.

Identity Authentication

USCIS uses a third-party, Identity Proofing (IdP) service to generate knowledge-based questions,[4] (i.e., a "quiz") based on commercial identity verification information, collected by third-party companies from financial institutions, public records, and other service providers. The information accessed by the IdP may include information, such as the individual's commercial transaction history, mortgage payments, or past addresses. An individual must correctly answer the quiz generated by the IdP in order to authenticate his identity and enable him to use E-Verify Self Check. In order to generate the quiz the IdP service collects basic PII from the individual including name, address of residence, date of birth, and optionally the individual's Social Security number (SSN).[5] Each individual will be asked a minimum of two and a maximum of four knowledge-based questions.

If an individual is not able to authenticate his identity, he will not be able to continue through E-Verify Self Check. There may be several reasons why an individual cannot pass identity authentication such as, insufficient commercial identity verification information on the individual for the IdP to generate a quiz, the individual has placed a fraud alert on his credit file, when there are multiple attempts to authenticate the individual, which may indicate possible fraud, or when the individual does not successfully pass the quiz. If the individual is able to answer the quiz questions correctly, the IdP authenticates his identity and returns a pass indicator to E-Verify, and the individual will continue through E-Verify Self Check. The IdP will send a pass indication, the name, date of birth, and SSN (if provided) to E-Verify. The IdP will not pass residence address to E-Verify. USCIS does not retain any PII from IdP sessions when an individual is unable to authenticate his identity or when an individual does not complete the second step of the E-Verify Self Check process, the E-Verify query. Regardless of whether the

[3] For additional information about the E-Verify process and possible outcomes of an E-Verify query such as a tentative non-confirmation, please see the E-Verify PIA published on May 4, 2010, available at http://www.dhs.gov/privacy.
[4] A knowledge-based question is one that is generated from public record information for example, identifying previous addresses from a list of addresses or the name of the bank that provided a car loan to the prospective employee.
[5] E-Verify Self Check will require individual to authenticate their identity through the IdP and providing a SSN enhances the ability of the IdP to generate knowledge-based questions. Since E-Verify Self Check aims to make itself accessible to any individual who wants to check his own work authorization status, DHS determined collection SSN on a voluntary basis would make E-Verify Self Check accessible to more individuals.

individual passes the identity assurance quiz, USCIS retains neither the questions generated by the IdP, nor the answers provided by the individual.

The IdP sends E-Verify Self Check a transaction number, a pass/fail indicator, the date and time of the transaction, and any applicable error code(s) to E-Verify, to facilitate troubleshooting and system management and improvement so that USCIS may keep statistics on how many individuals are able to authenticate through the IdP and consequently use E-Verify Self Check.

The Fair Credit Reporting Act (FCRA) requires the IdP to retain the fact of an inquiry. The IdP maintains the time/date stamp and inquiry type (credit check, identity check, etc.) so that the inquiry is noted in the individual's credit record and can be audited at a later date. Under FCRA, an individual has the right to know who has reviewed his credit report and the individual can place a fraud alert on his credit file. The E-Verify Self check inquiry is an identity check, and therefore will not affect an individual's credit score. Further, these types of inquiries are not shown to third parties who may request copies of credit reports. The IdP also maintains an audit log of all identity verification transactions. The audit log includes information submitted by the user (name, address, date of birth, SSN (if provided), the questions asked of the user, whether the user correctly answered the questions, the scores generated during the identity proofing process, and the business rules that were triggered during the transaction. These audit logs are maintained by the IdP service to conduct system management and to generate customer usage statistics.

E-Verify Query

Upon identity authentication, the individual moves to step 2: an E-Verify query to confirm current work authorization status. The IdP passes the name, date of birth, and SSN (if provided) to E-Verify Self Check (these data elements cannot be altered) to ensure that the information belongs to the individual who originally passed the identity authentication step. The individual will be required to enter additional information based on the documentation he would present to an employer for the Form I-9 process. The additional information collected from an individual depends on his citizenship status and the document chosen to present for work authorization. This could include: citizenship status; Alien Number (if non-citizen); passport number; Form I-94 number; and/or lawful permanent resident card or work authorization document (EAD) number. This represents the same information that is collected for the Form I-9 process and the basic E-Verify query.

E-Verify Self Check will query E-Verify through a web service connection and will present either that the information matched government records and that E-Verify would have found them work authorized, or that the information is a possible mismatch to government records. If the individual receives a "Possible mismatch with SSA/Immigration Information" response, E-Verify Self Check will provide guidance on how to correct potential errors in the records. The individual will be asked whether he would like to resolve the mismatch or not. If the individual chooses not to resolve the mismatch E-Verify will close the case. If the individual decides to resolve the SSA mismatch, a form will be generated that contains the individual's first and last name, the date and time of the E-Verify query, the E-Verify case number, and detailed instructions on how to resolve the mismatch. If the individual decides to resolve an Immigration Information mismatch, E-Verify Self Check provides instructions to contact E-

Verify Customer Contact Office (CCO) to speak to a status verification representative who will assist in the correction of immigration records 72 hours after the person's initial query. If the representative is unable to correct the record, the individual will be advised of actions necessary to correct the error.

USCIS maintains a record of the E-Verify query including the individual's name, date of birth, SSN, work authorization documentation information, the query result, and an E-Verify case number. This is consistent with how E-Verify queries initiated by authorized employers are maintained in E-Verify.[6]

Privacy Risks and Mitigation Strategies

DHS is using the services of a third-party IdP to authenticate identity for E-Verify Self Check, which presents privacy risks including the potential for an individual to inaccurately assume that DHS collects and maintains commercial identity verification information as well as the risk that an individual may not be able to authenticate his identity using the IdP. The main benefit of the Self Check program is to facilitate the identification and correction of potential errors in federal databases that provide inputs into the E-Verify system, thereby improving the E-Verify process for both the employee and the employer. Therefore, while there are risks to using a third-party IdP, overall DHS believes E-Verify Self Check benefits the privacy of individuals. Prior to the introduction of the E-Verify Self Check program, individuals did not have the ability to identify potential issues associated with his or her work authorization status until after receiving adverse notification from employers. Accordingly, the USCIS developed E-Verify Self Check to provide a vehicle to individuals to proactively check work authorization status prior to the employer conducting the E-Verify query.

DHS is using the services of a third-party IdP to authenticate identity. The IdP uses commercial identity verification information collected by third-party companies from financial institutions, public records, and other service providers. This commercial identity verification information does not belong to DHS nor is such information collected or retained by DHS. Nevertheless, there is a risk that an individual seeking to make use of E-Verify Self Check may inaccurately assume that this information belongs to and is collected and retained by DHS. In order to mitigate this risk, the E-Verify Self Check secure web portal user interface uses unique branding such as different color scheme and screen layout and messaging on the portal so that the user understands when he is interacting with DHS and when he is interacting with the IdP. Directional guidance also explains why the IdP is collecting the information, how the information is being used, and offers the user a way to exit the E-Verify Self Check service and delete his or her information before the identity authentication takes place.

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 a quiz if sufficient data pertaining to an individual cannot be located or when the individual has placed a lock on his 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

[6] See the E-Verify Program PIA and E-Verify System of Records Notice July 22, 2013, (78 FR 43893), for additional information about the information that may be accessed, stored, and retained during an E-Verify query.

hire, USCIS provides information on how to visit an SSA 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 is also advised to check the information at the various credit bureaus through a free credit check site.

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?

IIRIRA required DHS establish a Basic Pilot Program with voluntary participation by employers who could use this system to determine whether newly hired employees are authorized to work in the United States. This program was subsequently renamed the E-Verify program. Specifically,[7] Section 404(d) requires that the system be designed and operated to maximize the reliability and ease of use, enabling DHS to offer enhanced services to improve the reliability of the records used by E-Verify for work authorization. The authority provided by IIRIRA extends to the E-Verify Self Check, which is an enhancement to the E-Verify program. E-Verify Self Check is designed to improve the reliability of records by allowing individuals to check their work authorization status and correct any errors in their records prior to employment.

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

DHS/USCIS-013, E-Verify Self Check System of Records, February 16, 2011, (76 FR 9034) applies to E-Verify Self Check and DHS/USCIS-010, E-Verify System of Records, July 22, 2013, (78 FR 43893).

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

Yes. The system security plans (SSP) and Certification and Accreditation (C&A) were completed on March 21, 2011.

[7]The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), P.L. 104-208, Note: Sections 401-405 dated September 30, 1996.

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

Yes. DHS maintains a record of the E-Verify query and response to the query conducted via Self Check for 10 years in accordance with NARA retention schedule N1-566-08-7.

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 was approved on February 28, 2011.

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.

E-Verify Self Check is a two-step process: 1) identity authentication of the individual; and 2) an E-Verify query to confirm the individual's current work authorization status.

Identity Authentication

The first step, identity authentication uses a third-party, IdP service to generate a quiz based on commercial identity verification information. The information accessed by the IdP may include, information such as the individual's commercial transaction history, mortgage payments, or past addresses. An individual must correctly answer the quiz generated by the IdP in order to authenticate his identity and enable him to use E-Verify Self Check. In order to generate the quiz the IdP service collects basic PII from the individual including name, address of residence, date of birth, and optionally the individual's SSN.

If an individual is not able to authenticate his identity, he will not be able to continue through E-Verify Self Check. If the individual is able to answer the quiz questions correctly, his identity is authenticated, a pass indicator is returned to E-Verify, and the individual will continue through E-Verify Self Check. E-Verify will receive a pass indication and the name, date of birth, and SSN (if provided). Residence address will not be passed to E-Verify. USCIS does not retain any PII from IdP sessions when an individual is unable to authenticate his identity or when an individual does not complete the second step of the E-Verify Self Check process, the E-Verify query. Regardless of whether the individual passes the identity assurance quiz, USCIS retains neither the questions generated by the IdP, nor the answers provided by the individual.

The IdP sends E-Verify Self Check a transaction number, a pass/fail indicator, the date and time of the transaction, and any applicable error code(s) to E-Verify, to facilitate troubleshooting and system management and improvement so that USCIS may keep statistics of how many individuals are able to authenticate through the IdP and consequently use E-Verify Self Check.

The FCRA requires the IdP to retain the fact of an inquiry. The IdP maintains the time/date stamp and inquiry type (credit check, identity check, etc.) so that the inquiry is noted in the individual's credit record and can be audited at a later date. Under FCRA, an individual has the right to know who has reviewed his credit report and the individual can place a fraud alert on his credit file. The E-Verify Self check inquiry is an identity check, and therefore will not affect an individual's credit score. Further, these types of inquiries are not shown to third parties who may request copies of credit reports. The IdP also maintains an audit log of all identity verification transactions. The audit log includes information submitted by the user (name, address, date of birth, SSN (if provided), the questions asked of the user, whether the users got the answers correct, the scores generated during the identity proofing process, and the business rules that were triggered during the transaction. These audit logs are maintained by the IdP service to conduct system management and to generate customer usage statistics.

E-Verify Query

Upon identity authentication, the individual moves to step 2: an E-Verify query to confirm current work authorization status. The IdP passes the name, date of birth, and SSN (if provided) to E-Verify Self Check (these data elements cannot be altered) to ensure that the information belongs to the individual who originally passed the identity authentication step. The individual is required to enter additional information based on the documentation he would present to an employer for the Form I-9 process. The additional information collected from an individual depends on his citizenship status and the document chosen to present for work authorization. This could include: citizenship status; Alien Number (if non-citizen); passport number; Form I-94 number; and/or lawful permanent resident card or EAD number. This represents the same information that is collected for the Form I-9 process and the basic E-Verify query.

E-Verify Self Check will query E-Verify through a web service connection and will present either that the information matched government records and that E-Verify would have found them work authorized, or that the information is a possible mismatch to government records. If the individual receives a "Possible mismatch with SSA/Immigration Information" response, E-Verify Self Check provides guidance on how to correct potential errors in the records. The individual is asked whether he would like to resolve the mismatch or not. If the individual chooses not to resolve the mismatch E-Verify will close the case. If the individual decides to resolve the SSA mismatch, a form will be generated that contains the individual's first and last name, the date and time of the E-Verify query, the E-Verify case number, and detailed instructions on how to resolve the mismatch. If the individual decides to resolve an Immigration Information mismatch, E-Verify Self Check provides instructions to contact E-Verify CCO to speak to a status verification representative who will assist in the correction of immigration records 72 hours after the individual's initial query. If the representative is unable to correct the record, the individual will be advised of actions necessary to correct the error.

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

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

As detailed in Section 2.1, sources of information for E-Verify Self Check include: 1) the individual seeking to verify his work authorization status, 2) the third-party IdP service for identity verification, and 3) information contained in federal databases (SSA, DHS, and DOS) for the E-Verify basic query. The IdP uses commercial identity verification information, collected by third-party companies from financial institutions, public records, and other service providers

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 service for identity authentication. The IdP collects name, date of birth, address of residence, and SSN (if provided) in order to generate a quiz based on commercial identity verification information. FCRA requires the IdP to retain the fact of an inquiry. Accordingly, the IdP maintains the time/date stamp and inquiry type (credit check, identity check, etc.) so that the inquiry is noted in the individual's credit record and can be audited at a later date. The E-Verify Self check inquiry is an identity check, and therefore will not affect an individual's credit score. The IdP also maintains an audit log of all identity verification transactions. Audit logs are maintained by the IdP service to conduct system management and to generate customer usage statistics. The audit log includes information submitted by the user (name, address, date of birth, SSN (if provided), the questions asked of the user, whether the user answered the questions correctly, the scores generated during the identity proofing process, and the business rules that were triggered during the transaction.

2.4 Discuss how accuracy of the data is ensured.

The main benefit of E-Verify Self Check is to facilitate the identification and correction of potential errors in federal databases that provide inputs into the E-Verify System. In terms of accuracy of the information used by E-Verify Self Check, the initial data used in the E-Verify Self Check is provided by the individual and assumed to be accurate and further identity authentication is performed through the IdP service. The IdP uses commercial identity verification information from financial institutions, public records, and other service providers. 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 or her identity due to inaccurate information maintained by the IdP, he or she is advised to check his or her information at the various credit bureaus through a free credit check site.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: In order to use the E-Verify Self Check service, an individual must first pass identity authentication. It is possible that some individuals will not be able to use E-Verify Self Check because their identity cannot be authenticated. There are several reasons why this could happen. 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 and therefore there is insufficient information in which to develop questions to authenticate, or possibly an individual is attempting to illegitimately access the E-Verify database.

Mitigation: 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. 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 not deny anyone the ability to be work authorized through E-Verify, and there are still avenues available to the US workforce to check on the accuracy of their SSA and DHS records.

Privacy Risk: There is a potential risk that more information than is necessary will be collected through E-Verify Self Check.

Mitigation: The USCIS Verification Division Privacy Office and the E-Verify Self Check program underwent an analysis to determine which data elements were relevant and necessary for the purposes of facilitating identity verification and the E-Verify query by an individual seeking information on his work authorization status. For example, E-Verify Self Check will require individuals to authenticate their identity through the IdP, and providing a SSN enhances the ability of the IdP to generate knowledge-based questions. Since E-Verify Self Check aims to make itself accessible to any individual who wants to check his own work authorization status, DHS determined collection SSN on a voluntary basis would make E-Verify Self Check accessible to more individuals.

Privacy Risk: DHS is using the services of a third-party IdP to authenticate identity. The IdP uses commercial identity verification information collected by third-party companies from financial institutions, public records, and other service providers. This commercial identity verification information does not belong to DHS, nor will such information be collected or retained by DHS. Nevertheless, there is a risk that an individual seeking to make use of E-Verify Self Check may inaccurately assume that this information belongs to and is collected and retained by DHS.

Mitigation: The E-Verify Self Check secure web portal user interface uses unique branding such as different color schemes and screen layout and messaging on the portal so that the user understands when he or she is interacting with DHS and when he or she is interacting with the IdP. Directional guidance also explains why the IdP is collecting the information, how the information is being used, and

offers the user a way to exit the E-Verify Self Check service and delete his or her information before the identity authentication takes place.

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.

Individuals use E-Verify Self Check to determine their work authorization using the same process as E-Verify. E-Verify Self Check facilitates the identification and correction of potential errors in federal databases that provide inputs into the E-Verify system thereby improving the E-Verify process for both the employee and employer. In the first step of the E-Verify Self Check process, individuals must provide name, date of birth, address of residence, and SSN (optional) so that their identity can be verified.

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, the E-Verify Self Check service does not locate predictive patterns or anomalies in its operations or in the services it provides to its user base. The E-Verify Self Check process only verifies the identity of the individual using the system, and after identity verification, verifies work authorization in response to an individual inquiry. That information is matched against data in the E-Verify program. E-Verify Self Check does not allow users to perform predictive pattern analysis.

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

The information from the work authorization query part of E-Verify Self Check is available to USCIS staff tasked with the operation of the E-Verify Self Check service and is not shared within DHS except as required under the E-Verify data sharing requirements detailed under the Basic Pilot statute: specifically for law enforcement purposes as required by IIRIRA to prevent fraud and misuse of the E-Verify system. No additional sharing of E-Verify Self Check information is anticipated beyond that sharing described in the E-Verify PIA dated May 4, 2010.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the IdP will misuse the data collected during the identity verification process.

Mitigation: The IdP is contractually bound to only use the information collected from individuals for identity verification as defined by the Self Check business process, limited fraud identification and

prevention, and for the purposes as required by the FCRA. USCIS confirms the IdP compliance by ensuring all contract terms are adhered to through project management and compliance meetings throughout the term of the contract. We also provide guidance to users of Self Check to make us aware of any irregularities in their credit report as a result of using Self Check.

Privacy Risk: There is the potential for an individual to assume that DHS collects and maintains commercial identity verification information.

Mitigation: E-Verify Self Check secure web portal user interface uses unique branding such as a different color scheme, screen layout, and messaging on the portal so that the user understands when he or she is interacting with DHS and when he or she is interacting with the IdP. Directional guidance also explains why the IdP is collecting the information, how the information is being used, and offers the user a way to exit the E-Verify Self Check service and delete his or her information before the identity authentication takes place.

Privacy Risk: That DHS is relying on commercially-collected data that DHS does not validate directly with the individual.

Mitigation: Self Check is a voluntary program that individuals can use to assist in determining their employment authorization. There are no employment authorization determinations made through Self Check. The success or failure of a Self Check query will have no bearing on the official employer-run E-Verify query. The employer query is a brand new query at the time of hire. E-Verify Self Check uses commercially-collected data for the identity authentication only; nothing derogatory is indicated in the record nor is that information passed to DHS.

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.

Notice is provided in the Terms and Conditions, which the individual must accept before moving forward through the E-Verify Self Check process. The individual is also provided a Privacy Act notice before he or she begins identity authentication. At each step of the process an individual is given notice of the use, collection, and maintenance of his or her information. In addition, notice is provided through the DHS/USCIS-013 E-Verify Self Check System of Records SORN 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?

E-Verify Self Check is a voluntary program. E-Verify Self Check provides the individual with Terms and Conditions, which describe the individual's rights and options in using this program. There is no option to consent to only a portion of the program. If an individual does not wish to provide the required information, there are several opportunities to exit from the web site and choose not to participate. For example, an individual can exit the identity authentication process and nothing will be stored. An individual may also exit from E-Verify Self Check after successfully authenticating his identity and the information will be deleted and not stored by any DHS system.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: An individual seeking to make use of E-Verify Self Check may inaccurately assume that this information belongs to and is collected and retained by DHS.

Mitigation: The E-Verify Self Check secure web portal user interface uses unique branding including a different color scheme, screen layout, and messaging on the portal so that the user understands when he or she is interacting with DHS and when he or she is interacting with the IdP. Directional guidance explains why the IdP is collecting the information, how the information is being used, and offers the user a way to exit the E-Verify Self Check service and delete his or her information before the identity authentication takes place.

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 retains a log of IdP transactions consisting of transaction ID, pass/fail indicator, date and time of the transaction, and any applicable error code(s)in order to facilitate troubleshooting and system management so that USCIS may keep statistics of how many individuals are able to use the IdP and therefore E-Verify Self Check. If an individual does not pass identity authentication, all PII entered by the individual during the IdP session and any questions that may have been generated by the IdP are deleted at the end of the session (including if a user decides to end a session and not complete the Self Check process). If an individual passes identity authentication and completes the Self Check process, USCIS retains a record of the E-Verify query and the query result in E-Verify for 10 years in accordance with the NARA-approved records retention schedule identified in Section 1.4. This includes information such as, the individual's name, date of birth, SSN, work authorization documentation information, the query result, and E-Verify case number. USCIS maintains this information in order to assist the individual resolve potential errors in records contained in federal databases should the individual choose to do so prior to any formal, employer run E-Verify query process.

DHS is using the services of a third-party IdP to authenticate an individual's identity. The third-party IdP uses commercial identity verification information to generate the quiz. This commercial identity verification information does not belong to DHS nor will information from other sources relied upon by third-party provider be collected and/or retained by DHS. FCRA requires the IdP to retain the fact of an inquiry. The IdP maintains the time/date stamp and inquiry type (credit check, identity check, etc.) so that the inquiry is noted in the individual's credit record and can be audited at a later date. The E-Verify Self check inquiry is an identity check, and therefore will not affect an individual's credit score.

The IdP also maintains an audit log of all identity verification transactions. The audit log includes information submitted by the user (name, address, date of birth, SSN (if provided), the questions asked of the user, whether the users got the answers correct, the scores generated during the identity proofing process, and the business rules that were triggered during the transaction. These audit logs are maintained by the IdP service to conduct system management and to generate customer usage statistics. Audit logs of IDP transactions are first stored in the IDP Service's live database for three months. After three months, the audit logs are archived for an additional seven years. DHS does not have access to the IDP Service live database or the archives.

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: To mitigate this risk, USCIS minimizes PII retention to a record of the E-Verify query and query result for those individuals that successfully complete identity authentication and complete an E-Verify query. Further, regardless of whether the individual passes the identity assurance quiz, USCIS retains neither the questions generated by the IdP, nor the answers provided by the individual. USCIS retains a log of IdP transactions consisting of transaction ID, pass/fail indicator, date and time of the transaction, and any applicable error code(s)in order to facilitate troubleshooting and system management so that USCIS may keep statistics of how many individuals are able to use the IdP and therefore E-Verify Self Check.

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. Name, date of birth, address of residence, and SSN (if provided) will be collected for identity authentication purposes by a third-party IdP. This information sharing is covered under the Terms and Conditions document with the contracted third-party IdP service. The third-party IdP service is

barred from sharing any of the information provided under this service except as described under the terms and conditions of the contract in order to comply with an extensive set of legal requirements detailed in the FCRA that is protective of this type of information. The IdP does not share information with DHS except for the pass/fail of the identity authentication. As a result, this information cannot be and is not shared with any other elements of DHS, including the operators of the E-Verify Self Check service or other external entities.

Information from the work authorization query part of E-Verify Self Check 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 E-Verify Self Check mismatch resolution process, 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 DHS/USCIS-013 E-Verify Self Check SORN routine use "I" published on February 16, 2011, (76 FR 9034) authorizes the sharing specifically, "to a third-party commercial IdP under contract with the Department, but only the name, date of birth, address of residence, and SSN (if provided), for the purposes of authenticating an individual who is seeking to access USCIS E-Verify Self Check for employment eligibility. When there are multiple attempts to authenticate an individual, which indicates possible fraud, the DHS contract authorizes the IdP to notify the provider of the information of potential fraud and to terminate access to E-Verify Self Check. The IdP will share the fact of the inquiry with the appropriate credit bureau and monitor for potential fraudulent access in accordance with FCRA.

The IIRIRA statute that authorizes the operation of E-Verify requires DHS to share E-Verify information collected during E-Verify Self Check 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 the IIRIRA, which requires that USCIS determine whether an individual is work authorized, requires that USCIS uses 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 identity authentication information, the third-party data provider Terms and Conditions document, as well as the adherence to the Fair Credit Reporting Act, prohibit the re-dissemination of an individual's personally identifiable information.

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

The limited E-Verify systems dissemination to law enforcement agencies aligns with the IIRIRA requirement that USCIS prevent fraud and misuse of the E-Verify system. A log of extracts to law enforcement agencies is maintained and monitored by USCIS to ensure that sharing is in compliance with the Privacy Act and OMB requirements.

6.4 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: DHS is using the services of a third-party to authenticate identity for E-Verify Self Check presenting the potential for unauthorized use of an individual's name, date, of birth, address of residence, and SSN (if provided).

Mitigation: To mitigate risks associated with use of a third-party for identity authentication, DHS has a Terms and Conditions document with the contracted third-party IdP service to prevent unauthorized uses. The third-party IdP service is barred from sharing any of the information provided under this service except as described under the terms and conditions of the contract in order to comply with an extensive set of legal requirements detailed in the FCRA that is protective of this type of information.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their 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 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.

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

As noted in Section 7.1, E-Verify Self Check 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 as a mechanism to allow an individual to correct inaccurate or erroneous information.

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

E-Verify Self Check is a process that informs an individual that there may be an error in his or her records. E-Verify Self Check will allow the individual to correct his or her information, if that information is incorrect, in either DHS or SSA systems. If the information is incorrect, the individual will be given a DHS or SSA mismatch notice that will help to guide the individual through the correction process. The E-Verify Self Check correction process will follow the same procedures as described in the E-Verify PIA, dated May 4, 2010. This includes making the user aware of the mismatch, giving the user the opportunity to request further review of the mismatch, giving the user guidance of who to contact at SSA or DHS and what information will be needed to do so, and giving the user further information once contact is made with SSA and/or DHS, if more actions are needed. USCIS includes information in all its public outreach materials on E-Verify Self Check about the mismatch resolution process and how individuals can take advantage of the service to confirm the work authorization status or find out the steps needed to correct any record inaccuracies.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: An individual may be unable to authenticate his identity using the IdP because the IdP may not be able to generate knowledge-based questions or if sufficient data pertaining to an individual cannot be located or when the individual has placed a lock on his credit file. Additionally, an individual may not receive a passing score because the IdP information maintained is incorrect.

Mitigation: 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. USCIS will also advise the individual to check the information at the various credit bureaus through a free credit check site.

Section 8.0 Auditing and Accountability

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

The E-Verify Self Check IdP will rely on the services of a third-party data provider to authenticate an individual user's identity. The terms and conditions contained in the underlying USCIS contract with the identity assurance provider contains limitations on the use of personally identifiable information. The E-Verify Self Check process uses the technical, operational, and management controls to ensure that information in the system is protected and audited. Audit logs of the E-Verify Self Check verification will be kept in accordance with the E-Verify audit log procedures. The USCIS, Verification Division, Monitoring and Compliance Branch will have access to the E-Verify Self Check information to monitor the IdP process. This will include monitoring the usage patterns on a macro level (not individual-specific) to determine how many people are successfully authenticating their identity, and for those that

are not, what are the reasons why they are having problems (based on the error codes captured during the process). The E-Verify Self Check process was also designed to limit the amount of data asked for and provided by the individual to the absolute limit necessary to authenticate a person's identity and process a work authorization check.

Lastly, the terms and conditions that were established as part of our agreement with the third-party IdP is a legal agreement that prevents the sharing and/ or misuse of the data provided during its part of the operation of the E-Verify Self Check service. The third-party identity data provider must comply with an extensive set of legal requirements under FCRA that is protective of this type of information.

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

All employees with access to the E-Verify Self Check receive privacy training. The training for E-Verify Self Check employees is as described in the E-Verify PIA, dated May 4, 2010. Individuals verifying their work authorization through E-Verify Self Check will not be provided any formal privacy training but will be given sufficient privacy notice and information.

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

Limited numbers of Verification Division employees have access to E-Verify Self Check through the E-Verify program. This is described in the E-Verify PIA dated May 4, 2010. Anyone who has access to the internet will have access to the E-Verify Self Check program.

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. The E-Verify portion of E-Verify Self Check will follow the same sharing process as identified in the E-Verify PIA, dated May 4, 2010.

Responsible Official

Donald K. Hawkins
Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security
(202) 272-8030

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

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