Privacy Impact Assessment
for the

E-Verify Self Check Service

<<ADD Publication Date>>

Contact Point
Janice M. Jackson
Privacy Branch, Verification Division
United States Citizenship and Immigration Services
202-443-0109

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Citizenship and Immigration Services (USCIS) Verification Division has developed a new service called E-Verify Self Check. The E-Verify Self Check service is voluntary and available to any individual who wants to determine if they have any issues which may adversely affect their employment authorization through the E-Verify program. When an individual uses the Self Check service they will be notified that either their information matched the information contained in federal databases and they would be employment authorized or the information did not match. If the information did not match they will be given instructions on where and how to correct their records prior to the formal employer run E-Verify process. USCIS conducted this privacy impact assessment (PIA) because E-Verify Self Check will collect and use personal information and consequently requires a Privacy Impact Assessment.

Overview

Background

The E-Verify Program is a free and voluntary Department of Homeland Security (DHS) program implemented by the United States Citizenship and Immigration Services (USCIS) Verification Division and operated in collaboration with the Social Security Administration (SSA) to determine employment authorization. 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 employment authorization. In order to enable individuals to check their own employment authorization status prior to employment and facilitate correction of potential errors in federal databases that are inputs to the E-Verify process, USCIS developed the E-Verify Self Check service. Through the E-Verify Self Check web portal, individuals will be able to check their employment authorization status by first providing information to verify their identity in order to use the service, and subsequently, information on their I-9 employment documentation. Upon successful verification to the service, E-Verify Self Check will facilitate a query of E-Verify, which previously could only be conducted by authorized employers, and if the information provided by the individual matches the information contained in federal databases (SSA, DHS, DoS) a result of "work authorization confirmed." is displayed to the individual. If the information does not match, the individual will be provided with instructions on how to facilitate correction of potential errors in records contained in federal databases

prior to the formal, employer run E-Verify process.[1] The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) provides the statutory authority for E-Verify and by extension for the E-Verify Self Check process. This PIA update describes the new E-Verify Self Check service. Additionally, on May 4, 2010, E-Verify published a Privacy Impact Assessment (PIA) to describe the E-Verify program.

E-Verify Self Check Process

E-Verify Self Check service involves a two-step process, 1) identity verification and 2) a basic E-Verify query to identify current employment authorization status. The first step, identity verification utilizes a third party Identity Proofing (IdP) service to generate knowledge-based questions from public record information such as credit records that an individual must correctly answer in order to authenticate to use the E-verify Self Check service. The IdP service collects basic personal information from the individual including name, address, and date of birth. This information will be retained by the third-party provider in an audit log, however it will not be retained by DHS,. The individual may also opt to provide their Social Security number (SSN) to increase the likelihood of the IdP's ability to generate knowledge based questions. Each individual will be asked a minimum of two and a maximum of four questions. If there is not enough public data to generate two questions, the individual will not be able to verify his identity and will not be able to continue in the process. The third-party IdP scores the answers to the questions and returns a pass/fail indicator to USCIS. If the answers to the questions match the information contained in the commercial data base the individual will continue through the E-Verify Self Check process. If the individual fails identity verification they will not continue with the E-Verify Self Check process and a set of error codes will be returned to USCIS. (i.e., the reason for failure, failure to generate a quiz, incorrect answers, failure to connect with the service provider, etc.). All personal information entered by the individual and any questions that might have been generated by the third-party data IdP is terminated at the end of the session, nothing is stored or retained in E-Verify Self Check. The questions asked by the IdP and the answers provided by the individual are not provided to nor are they retained by USCIS. Only transaction ID and error codes are retained to facilitate troubleshooting and system management. Third-party data providers retain logs of access to personal information to comply with their legal obligations. Specifically, the Fair Credit Reporting Act (FCRA) requires that an inquiry be noted in a credit

[1] For additional information about the E-Verify process and possible outcomes of an E-Verfiy 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.

record; however the type of inquiry the IdP will perform will not impact an individuals' credit rating. The DHS contract for the IdP service permits the third-party provider to use the information provided through the E-Verify Self Check process in very limited ways such as internal fraud monitoring and prevention (to ensure that their system is not being misused or abused), and as required by federal law.

The second step in the E-Verify Self Check process is a basic E-Verify query to identify current employment authorization status. If an individual correctly answers the knowledge-based questions, the personal information provided to the IdP, name and date of birth, will persist and cannot be altered (to ensure that the information belongs to the individual who originally passed the identity assurance step), for a query of E-Verify to identify current employment authorization status. Next, the individual will be required to enter additional information based on the documentation they will present to an employer for processing in E-Verify. The information collected from an individual depends on their citizenship status and the document they choose to present for employment authorization and could include: name; SSN; citizenship status; Alien Number (if non-citizen); passport number; I-94 number; and /or permanent resident or employment authorization document (EAD) card number. This represents the same information that is collected for the basic E-Verify query and the only distinction is that the query is conducted on behalf of the individual for whom the record pertains versus the employer.

E-Verify Self Check will query E-Verify through a web service connection and return a response to the E-Verify Self Check service. E-Verify Self Check will then present a message on screen to the individual based on the response received from the basic E-Verify query. A message will be displayed to the individual that explains either that the information matched government records and that E-Verify would have found them work authorized or that the information did not match government records. Currently, E-Verify Self Check cannot correct records in the underlying databases that support the E-Verify program. If the individual receives a does not match response, E-Verify Self Check will provide guidance on how to correct potential errors in their records. A mismatch response from E-Verify Self Check could be either an SSA mismatch or a DHS mismatch. 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 has decided to resolve a DHS mismatch, they will be instructed to contact E-Verify Customer Contact Office (CCO) to correct their DHS records 72 hours after their initial query to correct their DHS records. At that time, the individual will be able to speak directly to a status verification representative. If the representative is unable

to correct the record, the individual will be advised of actions necessary to correct the error.

Guidance will be generated explaining the potential consequences and available actions they may want to take if an individual receives an SSA or DHS mismatch. If they do not select to resolve the mismatch, E-Verify Self Check will close the case. The record of the work authorization query will be retained in the VIS transactional database regardless of results.

Privacy Risks and Mitigation Strategies

To ensure that individuals using E-Verify Self Check understand that the identity authentication is conducted by a third party and is separate from the E-Verify program, the Self Check service contains unique branding and directional guidance identifying the entity collecting the information. No information displayed or supplied to E-Verify Self Check during the IdP portion will be accessible to nor retained by DHS.

There may be instances when individuals are unable to verify using the third party IdP service. This may result because no questions could be generated, such as individuals who have placed a lock on their credit file or may not have enough data or the data is incorrect. Individuals unable to authenticate through the E-Verify Self Check process, who still want to determine their work authorization status prior to hire, will be given information on how to visit an SSA field office, access their Social Security yearly statements, call USCIS, or submit a Freedom of Information Act (FOIA) request to access their work authorization records. They will be advised to check their information on the various credit bureaus through free credit check sites.

The Self Check program will help to mitigate many of the risks identified in the E-Verify program. The information collected for Self Check is the same information collected for E-Verify from the Form I-9. If there is an error in their data the Self Check program will provide information to individuals on how to correct their information prior to being hired by an E-Verify employer. This will help to reduce the number of Tentative Non-confirmations received through E-Verify. Additionally, if the individual used the Self Check program and found that their information did not match, and it was corrected by the individual prior to an E-Verify employer running an E-Verify query the employer would not know that there were any issues with the individual's records or documents.

The Self Check process collects information required for the authentication, which may include the social security number of the individual seeking to use the Self Check service. Only necessary information is provided to the third party to

verify identity during the authentication portion. The use of the social security number is optional. The social security number provides an additional means by which matching can be made. No additional information other than that provided by the individual is used in the matching process.

The third party data provider is restricted on how the information provided to them may be used. The terms and conditions of the agreement restricts the third party from sharing any of the data provided through Self Check with any entities (including DHS) and may only use the data for internal fraud monitoring and prevention which ensures that their system is not being misused or abused, and as required by federal law.. Additionally, the third party data provider must comply with the Fair Credit Reporting Act statute, which restricts use and requires protection of this information.

Section 1.0 Authorities and Other Requirements

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

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), requires the government provide for the establishment of 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.[2] Section 404(d) requires the system be designed and operated to maximize its reliability and ease of use, which allows the program to offer enhanced services to insure the reliability of the records used by E-Verify for employment authorization. The authority under the basic Pilot program extends to the E-Verify Self Check for this purpose, since E-Verify Self Check is designed to increase the reliability of records and to increase the ease of use of the E-Verify system. The 2010 Congressional appropriation of Funds (H.R. 2892) for E-verify requires that E-Verify create the E-Verify Self Check service to give U.S. workers the ability to check their work authorization status prior to being hired, which will enhance the reliability of the E-Verify program.

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

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

The Self Check Process SORN, which is being published concurrently with this PIA.

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

The Authority to Operate (ATO) is expected to be awarded on March 1st 2011 for the E-Verify Self Check project. This system will comply with DHS Management Directive 4300. As this is a new project, the Certification & Accreditation (C&A) and System Security Plan (SSP) are currently under development but will be produced and approved prior to go live on March 18, 2011.

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

Currently, there is no records retention schedule. The retention schedule is currently under development with NARA and this PIA will be updated when the retention schedule has been finalized. We are proposing that the retention schedule be for one (1) year in order to allow time for management analysis and proper reporting.

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.

An OMB Control Number will be assigned at a future time once the Office of Management and Budget approves the collection of this information under the Paperwork Reduction Act.

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, identity verification and employment authorization status. The first step of the process is the identity verification. The E-Verify Self Check application will use a commercial identity assurance service provider (IdP), customized as the DHS IdP Service, to verify an individual's identity. The IdP will collect information about the individual who has elected to use E-Verify Self Check. The information collected for the identity verification portion of Self Check will be as follows:

Name

Social Security Number (Optional)

Date of birth

Mailing address

The third-party data provider will then query various public databases returning between two and four identity based identity assurance questions. The individual will have to answer the questions correctly in order to proceed with employment eligibility status verification. These questions may ask previous addresses, phone numbers, financial account information, court record information, or other personal or financial based questions. The number of questions presented is based on the amount of public data available on the individual and the accuracy of the answers provided by the individual for each subsequent question.

The questions asked by the IdP and the answers provided by the individual are not provided to nor retained by USCIS. Only transaction ID and error codes are retained to facilitate troubleshooting and system management. Third-party data providers retain logs of access to personal information to comply with their legal obligations. The contract for identity proofing permits them to use this information only in very limited ways such as fraud monitoring and prevention (i.e. internal monitoring of their system use to ensure that it is not being misused or abused), and as required by federal law. The Fair Credit Reporting Act requires that an inquiry be noted to their credit record, but this will not affect their credit rating scores as the law states that inquiries of this type do not affect a credit rating.

There may be instances when individuals are unable to verify their identity using the third party IdP service because no questions could be generated. This may occur when an individual has placed a lock on their credit file, may not have enough data, or the data may be incorrect. Individuals unable to verify their identity through the E-Verify Self Check process, who want to determine their work

authorization status prior to hire, will be given guidance on how to visit an SSA field office, access their Social security statement online, call USCIS, or submit a Freedom of Information Act (FOIA) request to access their work authorization records. In addition, individuals will be advised to verify their information on the various credit bureaus through free credit check sites.

If the answers to the questions match the information contained in the commercial data base the individual will continue through the E-Verify Self Check process.

After the individual has verified their identity they will be redirected to the E-Verify Self Check screen to begin the E-Verify Self Check process. The individual's name and date of birth entered during identity verification is automatically pre-populated in E-Verify Self Check. This information will be unchangeable to ensure that the information represents the individual who originally passed the identity verification step. Next, the individual will be required to enter additional information that is used to determine employment authorization through the E-Verify process. This process is the same process as the basic E-Verify query and is described in the E-Verify PIA, dated May 4, 2010. The information that will be collected for the E-Verify Self Check query will come from the same sources as a query run by an E-Verify employer. The information collected depends on the citizenship and document chosen, but could include:

Name (required)

Social Security Number (required)

Citizenship Status (required)

Document type (required)

Alien Number

Passport Number

I-94 Number

Employment Authorization Document Card Number

Permanent Resident Card Number

A response will be generated from the information that was submitted by the individual. E-Verify Self Check will then present a screen to the individual based on the response received from E-Verify. A message will be displayed to the individual

that explains either that the individual provided information that matched government records and that E-Verify would have found them work authorized OR that the individual provided information that did not match government records. The individual will have the option to correct the error or not correct the data mismatch. If they select to correct the mismatch, the message will contain the first and last name, the date and time of the E-Verify query, the E-Verify case number, and guidance on how to resolve the mismatch

A mismatch response from E-Verify Self Check could be either an SSA mismatch or a DHS mismatch. If the individual decides to resolve the SSA mismatch, a form will be generated that contains guidance personalized for the individual directing them to an SSA Field Office. If the individual has decided to resolve a DHS mismatch they will be instructed to contact E-Verify Customer Contact Office (CCO) 72 hours after their initial query to correct their DHS records. The individual will speak directly to a status verification representative. If the SVO representative is unable to correct the record, the individual will be advised of actions necessary to correct the error

If the individual elects not to resolve an SSA or DHS mismatch, guidance will be generated explaining the potential consequences and available actions they may want to take. If they select not to resolve the mismatch, E-Verify Self Check will close the case. The record of the work authorization query will be retained in the VIS transactional database regardless of results.

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

All information used for Self Check is collected directly from the individual who wants to verify their employment authorization. Based on the personal information provided by the individual, a third-party data provider will perform a series of fraud-related checks to ascertain whether the individual has been reported as the victim of identity theft, or if they have provided an SSN, whether the SSN they have provided is valid. These checks are done by using the information provided and determine whether it matches information or records that exist in their fraud related databases. These fraud related databases are populated with confirmed instances of identity fraud and are checked to ensure that an imposter is not trying to run a E-Verify Self Check query posing as someone else.

Next the third-party data provider, will query various public databases such as credit bureaus, LexusNexis, public records, and will return two to four knowledge-based authentication questions which will be displayed to the individual. These

questions may ask about previous addresses or phone numbers, financial account information, court record information, previous employers, or other publicly accessible data from a variety of public data sources. The individual will have to answer all questions correctly in order to proceed with employment eligibility verification in E-Verify. The number of questions presented is based on the amount of public data available on the individual and will be between 2-4 questions per individual.

Upon successful completion of the IdP, the individual will be allowed to proceed to the second step of the process, which is the actual check of work authorization status through E-Verify Self Check.

At this point, the individual will provide additional information so that the E-Verify program can verify the employment authorization. The process for this is the same as described in the E-Verify PIA, dated May 4, 2010.

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

The data provided to the DHS IdP service is used to verify the identity of the individual user of the Self Check System. Individuals who elect to utilize Self Check will first have to provide basic information to verify their identity. The data elements that must be provided are: name, date of birth, address, and optionally, social security number. The IdP service will then verify identity by generating a list of questions. If the questions are answered correctly the individual will be allowed to advance to the next step of the process which is to check their employment authorization through E-Verify.

The information that is required and the answers provided for the identity verification portion of the Self Check program is used only by the third party and is not collected nor maintained in the E-Verify program or any other government database.

Based on the personal information and any other additional data collection from the individual, the IdP will perform a series of fraud-related checks to ascertain whether an individual has been reported as the victim of identity theft or if they have provided an SSN, whether the SSN they have provided is valid. Next the third-party data provider will query various public databases, and will return several knowledge-based authentication questions which will be displayed to the individual by the IdP service. These questions may ask about previous addresses or phone numbers, financial account information, court record information, previous employers, or other publicly accessible data from a variety of public data sources.

The individual will have to answer a set of questions correctly in order to proceed with employment eligibility verification through E-Verify Self Check. The number of questions presented is based on the amount of public data available on the individual and will be between 2-4 questions per individual.

The questions asked and the answers provided by the individual are not provided to USCIS. USCIS does not retain any personally identifiable information in its Self Check DHS IdP logs. Only transaction ID and error codes are retained to facilitate troubleshooting and system management. Third-party data providers retain logs of access to personal information in order to comply with their legal obligations to protect personally identifiable information in their possession per the Fair Credit Reporting Act. The terms and conditions that define the contract for identity proofing permits them to use this information only in very limited ways such as fraud monitoring and prevention within their own database. The Fair Credit Reporting Act also mandates restrictions on the sharing of any data obtained by the third party data provider.

The third party data provider is under strict restrictions on how the data provided to them may be used that are based on the terms and conditions of the agreement that they signed with the government to provide this service. This includes the restriction to not share the data provided through Self Check with any other entities (including DHS) and to only use the data provided for internal fraud monitoring and prevention to ensure that their system is not being used, misused or abused as required by federal law. The third party data provider is also restricted by the Fair Credit Reporting Act statute and must comply with an extensive set of legal requirements that is protective of this type of information

The identity proofing process and the IdP service rely on data already in the possession of the third-party data provider. The third-party data provider scores the answers to the identity proofing questions and returns a Pass/Fail indicator to USCIS. If the individual fails identity proofing, only a set of error codes will be returned to USCIS. USCIS does not retain the questions, the individual's answers, or any identifying information supplied by individuals seeking verification. If the individual decides to cancel the identity proofing process during the session or if the session times out because of inactivity, all personal information entered by the individual and any questions generated by the IdP is neither stored or retained in E-Verify Self Check. If the answers to the questions match the information contained in the commercial data base the individual will continue through the E-Verify Self Check process. If the individual successfully passes identity proofing, the personal information typed in by the individual persists for the purpose of employment eligibility verification.

2.4 Discuss how accuracy of the data is ensured.

To use E-Verify Self Check, the individual first has to verify their identity. The initial data used in the E-Verify Self Check service is provided by the individual and assumed to be correct. The information provided by the individual is basic biographical information. The information provided by the individual is checked against third party commercial data sources to verify identity. The data provided by the third-party data provider is data that is public and already in existence. No measures are in place to ensure the data from the third-party data sources are accurate. USCIS makes no claims that the data obtained and used for identity verification is correct or complete.

If the individual failed the identity verification process they will not be allowed to use E-Verify Self Check. Instead, individuals who are interested in determining their work authorization status will be directed to view and correct their data via existing processes such as contacting SSA, USCIS or make a FOIA request, to make corrections.

If the individual successfully completes IdP the individual will be passed to E-Verify Self Check. At this point the individual will be provided a query screen similar to what is provided to the employer through E-Verify. The name and date of birth that the individual entered for the identity authentication stage is pre-populated from the identity verification query step. The individual will provide other information required by E-Verify, and prior to submitting the query the system will display a confirmation page for review and correction. After the query has been submitted it follows the standard E-Verify query process outlined in the E-Verify PIA dated May 4, 2010.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: In order to utilize the Self Check service an individual must first pass identity verification. It is possible that some individuals will not be able to use Self Check because they will not pass the identity verification. There are a 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 their identity could not be verified. Another reason could be that the information contained in the commercial data bases 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 data base.

Mitigation: The use of this program is voluntary. Even if the individual fails to pass the identity verification portion, that does not mean that they will not be employment authorized in E-Verify. Failure to pass identity verification will not deny anyone the ability to be employment authorized through E-Verify. In this first phase of the service if an individual does not pass the identity verification portion there is no formal process to address the inability to verify identity. However, information will be provided on ways to view and correct their work authorization records through existing government channels such as FOIA, SSA or USCIS service operations.

Privacy Risk: There is a potential risk that too much information is being collected through E-Verify Self Check and provided to a third party commercial data source. The information may include the social security number in addition to the other information required to verify identity.

Mitigation: Self Check provides only necessary information to the third party commercial data source to verify identity. The social security number provides an additional means by which matching of the submitted information will match information contained in the commercial data bases. The use of the social security number is optional. No additional information other than that provided by the individual is used in the matching process.

The third party data provider is under strict restrictions on how the data provided to them may be used that are based on the terms and conditions of the agreement that they signed with the government to provide this service. This includes the restriction to not share the data provided through Self Check with any other entities (including DHS) and to only use the data provided for internal fraud monitoring purposes. The third party data provider is also restricted by the Fair Credit Reporting Act statute and must comply with an extensive set of legal requirements that is protective of this type of information."

Privacy Risk: There is a potential risk that individuals using E-Verify Self Check will believe that the information used in the identity verification portion of E-Verify Self Check will be available to, and retained by the Department of Homeland Security.

Mitigation: The E-Verify Self Check system is designed to separate the information from the IdP portion of the process from the work authorization query. No information that is displayed or supplied to the E-Verify Self Check individual during the IdP portion will be accessible to DHS nor will it be retained by DHS. The E-Verify Self Check application also contains clearly separate branding and directional guidance for the IDP portion to ensure that the individual understands that his information is being sent to a third party identity provider for verification purposes and will not be displayed to or retained by the Department of Homeland Security.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Individuals will use Self Check to determine their employment authorization using the same process as E-Verify. In the first step of the Self Check process the individual must provide name, date of birth and address so that their identity can be verified. That information is provided to a third party commercial data source for authentication. The individual also has the option to provide their social security number. The use of the social security number increases the probability that a match can be made.

After the identity verification is complete the individual will be passed to E-Verify Self Check. At this point the individual will be provided the basic E-Verify query screen. The name and date of birth that the individual had entered for their successful identity verification is pre-populated for the E-verify query. The individual will provide other information required by E-Verify. After the query has been submitted it follows the standard E-Verify query as outlined in the E-Verify PIA dated May 4, 2010.

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 its provides to its user base. The Self Check process will only verify identity of the individual using the system and after identity verification will verify employment authorization in response to user inquiry. That information will be matched against data in the E-Verify program. Once this Self Check process takes place, no user accounts will be created and no predictive pattern analysis will be performed.

3.3 Are there other components with assigned roles and responsibilities within the 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: The privacy risks for Self Check are identical to those described in the E-Verify PIA dated May 4, 2010.

Mitigation: Mitigation of these privacy risks will be in accordance with E-Verify PIA, dated May 4, 2010.

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.

Self Check is a voluntary program. Notice is provided in the Terms and Conditions, which the individual must accept before moving forward through the Self Check process. The individual is also directed to the DHS Privacy notice. At each step of the process an individual is given notice of the use, collection and maintenance of their information.

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

Self Check is a voluntary program. The Self Check individual is provided Terms and Conditions, which describes 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 chose not to participate, at which point their information will be deleted and not stored by any DHS system.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There are no privacy risks associated with notice or consent. Self Check is a voluntary program that individuals decide whether or not they want to participate.

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 does not retain any personally identifiable information in its Self Check IdP logs. Only transaction ID and error codes are retained in order to facilitate troubleshooting and system management. Third-party data providers retain logs of access to personal information in order to comply with their legal obligations to protect personally identifiable information in their possession per the Fair Credit Reporting Act. The contract for identity proofing permits them to use this information only in very limited ways such as fraud monitoring and prevention, and as required by the Fair Credit Reporting Act. This data is kept for one year and is also reflected as a soft inquiry on the individual's credit report for one year. A soft inquiry has no impact on credit score and can be seen only by the individual and the credit bureau. It is required by the Fair Credit Reporting Act to assist in monitoring access to credit files.

Currently, there is no records retention schedule. The retention schedule is currently under development with NARA and this PIA will be updated when the retention schedule has been finalized. We are proposing that the retention schedule be for one (1) year in order to allow time for management analysis and proper reporting. Until approval of the new retention schedule Self Check information will be retained indefinitely.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Until the new retention schedule is developed the information collected from the Self Check program must be retained indefinitely. The proposed schedule is to maintain the Self Check information for one (1) year.

Mitigation: Approved retention schedule through NARA.

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.

Information from the IdP process contained in E-Verify Self Check is provided to the IdP provider to conduct the IDP service. This information sharing is covered under the Terms and Conditions document with the contracted third party ID provider service. The third party ID provider service is barred from sharing any of the information provided under this service with any other entity under the terms and conditions of the contract and also must comply with an extensive set of legal requirements detailed in the Fair Credit reporting Act that is protective of this type of information. This information is not shared with any other elements of DHS, including the operators of the Self Check service. The data provider does not share information with DHS besides pass/fail.

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 described in the E-Verify PIA dated May 4, 2010.

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

The IIRIRA statute that authorizes the operation of E-Verify requires DHS to share E-Verify information collected during Self Check with Law Enforcement and the Social Security Administration (SSA). Sharing information with SSA is compatible with the original collection because the IIRIRA which requires that USCIS determine whether an individual is employment authorized using 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?

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.

Information from 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 employment authorized. The limited E-Verify systems information use by sharing with Law Enforcement agencies aligns with the IIRIRA requirement that USCIS prevent fraud and misuse of the E-Verify system. The information maybe re-disseminated for law enforcement purposes only.

A log of extracts 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: No risks specific to Self Check beyond those explained in the E-Verify PIA.

Mitigation: Mitigation steps are discussed in the E-Verify PIA.

Section 7.0 Redress

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

The Self Check IdP will provide an individual that has failed to verify their identity information on records correction at SSA and credit bureaus as well as refer them to redress available under the Fair Credit Reporting Act. The E-Verify portion of Self Check will follow the same process as identified in the E-Verify PIA, dated May 4, 2010.

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

The purpose of Self Check is to allow the individual to correct their information if that information is incorrect in either DHS or SSA systems. If the E-Verify information is incorrect the individual will be given a DHS or SSA mismatch notice which will help to guide them through the correction process. The Self Check correction process will follow the same procedure as described in the E-Verify PIA, dated May 4, 2010.

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

Self Check is a process for an individual to be informed that there may be an error in their records. Self Check will allow the individual to correct their 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 which will help to guide them through the correction process. The Self Check correction process will follow similar procedures as described in the E-Verify PIA, dated May 4, 2010.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: The Self Check process is essentially a program to provide redress. Therefore there is no associated privacy risk.

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 Self Check IdP will rely on third party data provider Terms and Conditions and contractual requirements and Plan of Action and Milestones (POAMs) for the identity assurance provider. The 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 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 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 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 identity data provider is a legal agreement that prevents the sharing and or misuse of the data provided during its part of the operation of the Self Check Service. The third party identity data provider must comply with an extensive set of legal requirements under the Fair Credit reporting act 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 Self Check will receive privacy training. The training for Self Check employees is as described in the E-Verify PIA, dated May 4, 2010. Individuals verifying their employment authorization through 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 determine who has access?

Limited numbers of Verification Division employees have access to 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 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?

All information sharing agreements are reviewed by the program manager, Privacy Branch Chief and counsel. The E-Verify portion of Self Check will follow the same sharing process as identified in the E-Verify PIA, dated May 4, 2010.

.

Responsible Officials

<<Janice M. Jackson, Acting Chief
Privacy Branch, Verification Division
United States Citizenship and Immigration Services>>
Department of Homeland Security

Approval Signature

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security