



PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.



Privacy Threshold Analysis (PTA)

Specialized Template for Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

| | | | |
|---------------------|---|----------------|----------------------------------|
| Form Number: | Form G-1499 | | |
| Form Title: | MyE-Verify (existing collection) – PRA renewal | | |
| Component: | U.S. Citizenship and Immigration Services (USCIS) | Office: | VERIFICATION DIVISION |

IF COVERED BY THE PAPERWORK REDUCTION ACT:

| | | | |
|----------------------------|-----------------------------------|--|--------------------------|
| Collection Title: | MyE-Verify | | |
| OMB Control Number: | OMB Control No.: 1615-0117 | OMB Expiration Date: | July 31, 2017 |
| Collection status: | Extension | Date of last PTA (if applicable): | December 28, 2012 |

PROJECT OR PROGRAM MANAGER

| | | | |
|----------------|--|---------------|---------------------------------|
| Name: | Matthew Wiggins | | |
| Office: | Product Development, Verification Modernization | Title: | Product Owner |
| Phone: | 202-443-0309 | Email: | Matthew.R.Wiggins@uscis.dhs.gov |

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

| | |
|--------------|-----------------|
| Name: | Matthew Wiggins |
|--------------|-----------------|



| | | | |
|---------|---|--------|---------------------------------|
| Office: | Product Development, Verification Modernization | Title: | Product Owner |
| Phone: | 202-443-0309 | Email: | Matthew.R.Wiggins@uscis.dhs.gov |

SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form

- a. Describe the purpose of the information collection or form. *Please provide a general description of the project and its purpose, including how it supports the DHS mission, in a way a non-technical person could understand (you may use information from the Supporting Statement).*

If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.

The E-Verify program allows employers to electronically confirm the employment authorization of newly hired employees by matching information provided by employees on the Form I-9, Employment Eligibility Verification, against existing information contained in the Verification Information System, a database that matches the information provided against the information contained by both the Social Security Administration (SSA) and the Department of Homeland Security (DHS).

The myE-Verify will allow employees to proactively engage with E-Verify through a suite of Web-based services. The features of myE-Verify are free and provides individuals a way to establish a secure account that facilitates an ongoing relationship between the user and U.S. Citizenship and Immigration Services (USCIS). myE-Verify lets individuals confirm that their records for employment eligibility are accurate. It also helps individuals protect their identity and informs them about their E-Verify employer's responsibilities and their rights in the E-Verify employment eligibility verification process.

The first myE-Verify feature is E-Verify Self Check. USCIS developed the E-Verify Self Check service to allow workers in the United States to enter data into the Verification Information System (VIS) to ensure that the information relating to their eligibility to work is accurate before beginning new employment. This will lead to a more reliable and accurate E-Verify system that works better for both employers and employees. It verifies their personal information against the same records E-Verify checks. Job seekers can confirm that their records are in order or, if a mismatch occurs, learn how to make updates.

The next functionality of myE-Verify will be the ability for individuals to create a secure account and access the Self Lock feature after using E-Verify Self Check. Below are brief descriptions of myE-Verify features:

- myE-Verify Accounts – allows the individual who completes the Self Check process to set up a secure account to access features.



| | |
|--|--|
| <ul style="list-style-type: none"> • Self Lock – empowers individuals to actively protect their Social Security Number (SSN) from use in employment related identity fraud by allowing the account holder to lock his or her SSN from use by anyone in E-Verify. • Case Tracker – lets employees follow the status of their own E-Verify case resolution. It allows the account holder to get detailed information and guidance about a contested Self Check case. • Document Expiration Reminders – allows an account holder to enter information about employment eligibility documents and set up expiration reminders. • Case History – It allows individuals to see where their information has been used in E-Verify and Self-check. It allows an account holder to view a modified VIS report to review details around use of his or her SSN in E-Verify to detect any instances of identity fraud. | |
| <p>b. List the DHS (or component) authorities to collect, store, and use this information. <i>If this information will be stored and used by a specific DHS component, list the component-specific authorities.</i></p> | |
| <p>The authority for the E-Verify program is contained in section 404 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) Public Law 104–208. 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.</p> | |

| 2. Describe the IC/Form | |
|--|--|
| <p>a. Does this form collect any Personally Identifiable Information” (PII¹)?</p> | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| <p>b. From which type(s) of individuals does this form collect information? <i>(Check all that apply.)</i></p> | <input checked="" type="checkbox"/> Members of the public (anyone who has a E-Verify account) <input checked="" type="checkbox"/> U.S. citizens or lawful permanent residents <input checked="" type="checkbox"/> Non-U.S. Persons. <input checked="" type="checkbox"/> DHS Employees |

¹ Personally identifiable information means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



| | |
|---|---|
| | <input checked="" type="checkbox"/> DHS Contractors <input checked="" type="checkbox"/> Other federal employees or contractors. |
| <p>c. Who will complete and submit this form? (<i>Check all that apply.</i>)</p> | <input checked="" type="checkbox"/> The record subject of the form (e.g., the individual applicant). <input type="checkbox"/> Legal Representative (preparer, attorney, etc.). <input type="checkbox"/> Business entity. <p style="padding-left: 40px;">If a business entity, is the only information collected business contact information?</p> <p style="padding-left: 80px;"><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <input type="checkbox"/> Law enforcement. <input type="checkbox"/> DHS employee or contractor. <input type="checkbox"/> Other individual/entity/organization that is NOT the record subject. <i>Please describe.</i> Click here to enter text. |
| <p>d. How do individuals complete the form? <i>Check all that apply.</i></p> | <input type="checkbox"/> Paper. <input type="checkbox"/> Electronic. (ex: fillable PDF) <input checked="" type="checkbox"/> Online web form. (available and submitted via the internet) Provide link: https://selfcheck.uscis.gov/SelfCheckUI/ . |
| <p>e. What information will DHS collect on the form? <i>List all PII data elements on the form. If the form will collect information from more than one type of individual, please break down list of data elements collected by type of individual.</i></p> | |
| <p>The creation of a myE-Verify account requires the collection and retention of the following data elements:</p> <ul style="list-style-type: none"> • User Name (established by the user) • Password (established by the user) • Mailing address (street address, city, state, zip code) • Email address and/or cell phone number <p>To check employment authorization using myE-Verify Self Check, a user will first enter minimal biographical information (name, address, date of birth, and optional SSN, alien number, and/or passport number). To authenticate the user's identity, the information will be sent to a 3rd party identity authentication service that will then generate a series of questions back to the user. The user</p> | |



will then have to correctly answer the identity authentication questions before continuing the process. The exact questions generated will be unique to each user. The following is a sample of the category of questions:

- Address;
- SSN State of issue;
- SSN last four digits;
- Phone Number;
- Employer;
- Household;
- Personal Property;
- Driver's License Number; and
- Credit questions relating to: Mortgage/ Home Equity Loan, Auto Loan, Personal Installment Loan, Student Loan, and Credit Accounts.

If the identity authentication process is successful, the user enters their citizenship status information, SSN, and document number(s) from documents showing their employment authorization. Drop-down menus will be provided for citizenship status and document selection. The system then transmits the data to SSA to compare the name and social security account number provided by the user against the records created by SSA at the time of enumeration, and maintained by SSA, to confirm (or not confirm) the validity of the information provided by the employee, including whether the individual's name and the SSN correspond to each other, and whether the social security account number provided is valid/invalid for employment. The results of the SSA records comparison are returned to the user via Self Check. If the user enters immigration information (e.g., Arrival Departure Record (I-94) number, Alien number, USCIS number), then the information is transmitted to DHS to compare the documents numbers provided by the user against DHS records. The results of the DHS records comparison are also returned to the user via Self Check.

The use of the case tracking functionality requires the collection of the following data elements. These elements are not stored by Self Check after the status inquiry is completed.

- Case Verification Number (provided by Self Check)
- Date of Birth

The use of Self Lock functionality requires the collection and retention of the following data elements:

- Social Security Number
- Three challenge questions and answers (these challenge questions will be used as part of the authentication procedure for individuals who call Status Verification Operations (SVO) to change their Self Lock preferences from locked to unlocked).

The use of E-Verify Case History reports requires the collection of the SSN and DOB. The information is not retained but re-entered with each new use in order to pull reports.

Document Expiration Reminders is a feature that allows an account holder to enter information about employment authorization documents and set up reminders. The information provided will be stored by the 3rd party account management service providers. The provided information will not be checked



against government records for accuracy and will not be used for any purpose aside from providing the account holder with document reminders pertaining to the information submitted by the user.

The following information is needed for the Document Expiration Reminders feature: Document Type (e.g., Employment Authorization Document, Permanent Resident Card, etc.); and Expiration Date.

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? *Check all that apply.*

- | | |
|--|---|
| <input checked="" type="checkbox"/> Social Security number | <input type="checkbox"/> DHS Electronic Data Interchange |
| <input checked="" type="checkbox"/> Alien Number (A-Number) | Personal Identifier (EDIPI) |
| <input type="checkbox"/> Tax Identification Number | <input type="checkbox"/> Social Media Handle/ID |
| <input type="checkbox"/> Visa Number | <input type="checkbox"/> Known Traveler Number |
| <input checked="" type="checkbox"/> Passport Number | <input type="checkbox"/> Trusted Traveler Number (Global |
| <input type="checkbox"/> Bank Account, Credit Card, or other | Entry, Pre-Check, etc.) |
| financial account number | <input checked="" type="checkbox"/> Driver's License Number |
| <input type="checkbox"/> Other. <i>Please list:</i> | <input type="checkbox"/> Biometrics |

g. List the **specific authority** to collect SSN or these other SPII elements.

The Illegal Reform and Immigrant Responsibility Act of 1996 (IIRIRA) required DHS to establish the 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, 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 service, which enhances 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. The authority for Self Lock is the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA). The Self Lock program and the collection of information associated are within the spirit and letter of the IIRIRA provisions (Subtitle A, Title IV, Div. C of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. 104-208, as amended (8 U.S.C.A. 1324a note)). Further, IIRIRA requires the E-Verify system to include appropriate administrative, technical, physical and procedural safeguards to detect and deter fraud or other misuse within the E-Verify system. The scope of Self Lock's identity theft protection is limited to use of SSN's within the E-Verify system for the protection of SSNs within the E-Verify program.



| | |
|---|--|
| <p>h. How will this information be used? What is the purpose of the collection? Describe why this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.</p> | |
| <p>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, so that their identity can be verified. Information collected for Self Lock is used to prevent an individual's SSN from being used in the E-Verify system without the individual's permission and thus prevent identity theft.</p> | |
| <p>i. Are individuals provided notice at the time of collection by DHS (<i>Does the records subject have notice of the collection or is form filled out by third party</i>)?</p> | <p><input checked="" type="checkbox"/> Yes. Please describe how notice is provided. E-Verify Self Check is a voluntary program. 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. The 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.</p> <p><input type="checkbox"/> No.</p> |

| 3. How will DHS store the IC/form responses? | |
|--|--|
| <p>a. How will DHS store the original, completed IC/forms?</p> | <p><input type="checkbox"/> Paper. Please describe. Click here to enter text.</p> <p><input checked="" type="checkbox"/> Electronic. Please describe the IT system that will store the data from the form. Some information will be stored in the Verification Information System.</p> <p><input type="checkbox"/> Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository.</p> |



| | |
|--|--|
| | <p>Click here to enter text.</p> |
| <p>b. If electronic, how does DHS input the responses into the IT system?</p> | <p><input type="checkbox"/> Manually (data elements manually entered). Please describe. Click here to enter text.</p> <p><input checked="" type="checkbox"/> Automatically. Please describe.</p> <p>All information for E-Verify Self Check will be collected electronically through a Web-based portal at https://selfcheck.uscis.gov/SelfCheckUI/. This method provides the most efficient means for collecting and processing the required data.</p> |
| <p>c. How would a user search the information submitted on the forms, <i>i.e.</i>, how is the information retrieved?</p> | <p><input checked="" type="checkbox"/> By a unique identifier.² <i>Please describe.</i> If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. These include SSN, Case verification number, Date of birth, Passport number, Alien number, Form I-94 number, and/or lawful permanent resident card or work authorization document (EAD) number, and email address. The identifier used is dependent on the user (the employee, SSA or IdP) or the document submitted.</p> <p><input type="checkbox"/> By a non-personal identifier. <i>Please describe.</i> Click here to enter text.</p> |
| <p>d. What is the records retention schedule(s)? <i>Include the records schedule number.</i></p> | <p>If an individual passes identity authentication and completes the Self Check process, 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. 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).</p> <p>The IdP also maintains an audit log of all identity verification transactions. The audit log includes information submitted by</p> |

² Generally, a unique identifier is considered any type of “personally identifiable information,” meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



| | |
|---|--|
| | <p>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.</p> |
| <p>e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?</p> | <p>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.</p> |
| <p>f. Is any of this information shared outside of the original program/office? <i>If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?</i></p> | |
| <p><input type="checkbox"/> Yes, information is shared with other DHS components or offices. Please describe. Click here to enter text.</p> <p><input checked="" type="checkbox"/> Yes, information is shared <i>external</i> to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe.</p> <p>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.</p> | |



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.

No. Information on this form is not shared outside of the collecting office.



Please include a copy of the referenced form and Privacy Act Statement (if applicable) with this PTA upon submission.



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

| | |
|---|---|
| Component Privacy Office Reviewer: | Sarita Rijhwani/Kristy Sawyer |
| Date submitted to component Privacy Office: | November 21, 2016 |
| Date submitted to DHS Privacy Office: | November 30, 2016 |
| Have you approved a Privacy Act Statement for this form? <i>(Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.)</i> | <input checked="" type="checkbox"/> Yes. Please include it with this PTA submission. <input type="checkbox"/> No. Please describe why not. Click here to enter text. There is an existing PA statement since this is PRA package renewal. USCIS Office of Privacy developed a Privacy Act Statement and is seeking OCC approval. |
| <p>Component Privacy Office Recommendation:</p> <p>The E-Verify program allows employers to electronically confirm the employment authorization of newly hired employees by matching information provided by employees on the Form I-9, Employment Eligibility Verification, against existing information contained in the Verification Information System, a database that matches the information provided against the information contained by both the Social Security Administration (SSA) and the Department of Homeland Security (DHS).</p> <p>The myE-Verify will allow employees to proactively engage with E-Verify through a suite of Web-based services. The features of myE-Verify are free and provides individuals a way to establish a secure account that facilitates an ongoing relationship between the user and U.S. Citizenship and Immigration Services (USCIS). myE-Verify lets individuals confirm that their records for employment eligibility are accurate. It also helps individuals protect their identity and informs them about their E-Verify employer's responsibilities and their rights in the E-Verify employment eligibility verification process.</p> <p>This is an existing collection that is being renewed since the current OMB approval expires on 7/31/2017. The collection is covered by existing privacy documents –</p> <p>PIAs: DHS/USCIS/PIA-030(e) myE-Verify, DHS/USCIS/PIA – 030(d) E-Verify Program DHS/USCIS/PIA-030(b) E-Verify Self Check</p> | |



SORNs:

DHS/USCIS-011 E-Verify Program, August 11, 2014, 79 FR 4852

DHS/USCIS-013 E-Verify Self Check, February 16, 2011, 76 FR 9034

DHS/ALL-037 E-Authentication Records, August 11, 2014, 79 FR 46857

[Click here to enter text.](#)



PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

| | |
|--------------------------------------|---------------------|
| DHS Privacy Office Reviewer: | Max Binstock |
| PCTS Workflow Number: | 1135686 |
| Date approved by DHS Privacy Office: | December 21, 2016 |
| PTA Expiration Date | December 21, 2019 |

DESIGNATION

| | |
|--------------------------------|--|
| Privacy Sensitive IC or Form: | Yes If "no" PTA adjudication is complete. |
| Determination: | <input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing SPII applies. <input checked="" type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Specialized training required. <input type="checkbox"/> Other. Click here to enter text. |
| DHS IC/Forms Review: | DHS PRIV has not received this ICR/Form. |
| Date IC/Form Approved by PRIV: | Click here to enter a date. |
| IC/Form PCTS Number: | Click here to enter text. |
| Privacy Act Statement: | New e(3) statement is required. Click here to enter text. |
| PTA: | New system PTA required. Click here to enter text. |
| PIA: | System covered by existing PIA If covered by existing PIA, please list: DHS/USCIS/PIA-030 E-Verify |



| | |
|---|---|
| | If a PIA update is required, please list: Click here to enter text. |
| SORN: | <p>System covered by existing SORN</p> <p>If covered by existing SORN, please list: DHS/USCIS-011 E-Verify Program, August 11, 2014, 79 FR 46852; DHS/ALL-037 E-Authentication Records System of Records, August 11, 2014, 79 FR 46857</p> <p>If a SORN update is required, please list: Click here to enter text.</p> |
| <p>DHS Privacy Office Comments:</p> <p><i>Please describe rationale for privacy compliance determination above.</i></p> | |
| <p>USCIS Privacy is submitting this PTA because myE-Verify will allow employees to proactively engage with E-Verify through a suite of Web-based services. myE-Verify lets individuals confirm that their records for employment eligibility are accurate. It also helps individuals protect their identity and informs them about their E-Verify employer’s responsibilities and their rights in the E-Verify employment eligibility verification process.</p> <p>PRIV finds that is a privacy sensitive system and a PIA is required because myE-Verify collects PII from members of the public, DHS employees and contractors, contractors working on behalf of DHS, and employees of other federal agencies.</p> <p>PRIV agrees with USCIS Privacy that the E-Verify PIAs provide adequate coverage. DHS/USCIS/PIA-030(b) discusses E-Verify Self Check, which enables any individual to check his own work authorization status prior to employment, and facilitates correction of potential errors in federal databases that provide inputs into the E-Verify process. DHS/USCIS/PIA-030(d) discusses the collection and verification of foreign passport COI through US-VISIT. DHS/USCIS/PIA-030(e) discusses myE-Verify, a voluntary service that provides individuals with features that foster greater insight and control into the handling of their PII in E-Verify and Self Check.</p> <p>PRIV finds that a SORN is required because myE-Verify retrieves information by a unique identifier. PRIV agrees with USCIS Privacy that the E-Verify Program SORN and E-Authentication SORN provide adequate coverage. DHS/USCIS-011 covers employment authorization information to employers participating in E-Verify and to individuals seeking to check employment eligibility under the INA. DHS/ALL-037 covers records about individuals who electronically authenticate their identities.</p> | |