PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether
a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSOnline and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.

PRIVACY THRESHOLD ANALYSIS (PTA)

Please complete this form and send it to the DHS Privacy Office.
Upon receipt, the DHS Privacy Office will review this form
and may request additional information.

SUMMARY INFORMATION

DATE **submitted for review: September 14, 2010**

NAME **of** Project**: E-Verify Self Check**

Name of Component: US Citizenship and Immigration Services

Name of Project Manager: Michael Mayhew

Email for Project Manager: michael.mayhew@dhs.gov

Phone number for Project Manager: 202 443-0021

TYPE **of Project:**

☒ **Information Technology and/or System**[*]

□ **A Notice of Proposed Rule Making or a Final Rule.**

□ **Other: <Please describe the type of project including paper based Privacy Act system of records.>**

[*] The E-Government Act of 2002 defines these terms by reference to the definition sections of Titles 40 and 44 of the United States Code. The following is a summary of those definitions:

- "Information Technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. See 40 U.S.C. § 11101(6).
- "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Note, for purposes of this form, there is no distinction made between national security systems or technologies/systems managed by contractors. All technologies/systems should be initially reviewed for potential privacy impact.

SPECIFIC QUESTIONS

1. Describe the project and its purpose:

Currently, individuals are verified through the E-Verify process after they have been hired by an E-Verify employer. Employees who receive a Tentative Non-Confirmation (TNC) may have to take time off from work to resolve an issues that led to the TNC. In some limited instances, employers do not follow E-Verify rules and they terminate employees rather than work with them to resolve the TNC. There is no capability for an individual to determine what the result of an E-Verify query would be, until they have been hired and run through the system by their new employer.

The Self Check Process will give workers the ability to check their own work authorization status by querying E-Verify's Verification Information System (VIS) at anytime from from any computer that has web access. This will allow employees to proactively address any issues that could lead to a TNC, thereby reducing the overal number of TNC's, as well as those leading to unlawful terminations.

The E-Verify Self Check process works in the same manner as the normal employer E-Verify process. An individual will submit the same information required for an E-Verify query and it will then be checked against VIS databases to determine the individual's work authorization status. This process has been described and approved as part of the E-Verify System of Records Notice (SORN) and Privacy Impact Assessments (PIA).

Before the Self Check process begins the individual must go through an identity proofing process to help ensure that the identifying information submitted actually relates to the individual submitting the query. The Self Check application will use a third party vendor that will collect certain identifying information such as the individuals name, date of birth, home address, and optionally the social security number and search various public databases returning a number of knowledge-based identity proofing questions to the individual. The optional use of the social security number will assist to help to identify individuals that may not have a significant credit history. These questions may concern previous addresses or phone numbers, financial account information, court record information, and other publicly accessible data. The individuals will be offered a number of questions, if they are able to respond to the questions in a satisfactory manner they will be allowed to proceed to the Self Check screen which will be pre-populated with the name entered during the identity proofing step. If they are unable to answer the questions satisfactorily they will not be able to proceed and run an E-Verify Self Check query and they must rely on the employer running the E-Verify query.

In later iterations of Self Check it is assumed that a process will be developed for individuals to have additional options to prove their identity if they are unable to successfully pass the identity proofing process using the knowledge-based questions.

2. Status of Project:

☒ This is a new development effort.

☐ This is an existing project.

Date first developed:

Date last updated:

3. **Could the project relate in any way to an individual?**[1]

☐ No. Please skip ahead to the next question.

☒ Yes. Please provide a general description, below.

It allows individuals to query their own work authorization status at anytime that is convenient for them. This allows them time to resolve potential issues before an employer runs their information through E-Verify and minimizes the likelihood that they will receive a TNC.

4. **Do you collect, process, or retain information on: (Please check all that apply)**

☐ DHS Employees

☐ Contractors working on behalf of DHS

☒ The Public

☐ The System does not contain any such information.

[1] Projects can relate to individuals in a number of ways. For example, a project may include a camera for the purpose of watching a physical location. Individuals may walk past the camera and images of those individuals may be recorded. Projects could also relate to individuals in more subtle ways. For example, a project that is focused on detecting radioactivity levels may be sensitive enough to detect whether an individual received chemotherapy.

5. **Do you use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs)**

□ No.

☒ Yes. Why does the program collect SSNs? Provide the function of the SSN and the legal authority to do so:

Collecting the SSN is part of the E-Verify process as described in the E-Verify PIA and SORN. The optional use of the social security number during the authentication process will assist to help to identify individuals that may not have a significant credit history.

6. **What information about individuals could be collected, generated or retained?**

The exact requirements have not yet been determined but it is expected that the application will collect some combination of name, date of birth, home address, and optionally the social security number as part of the authentication process. Other data elements are collected as described in the E-Verify PIA and SORN.

7. **If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]?**

☒ No. Please continue to the next question.

□ Yes. Is there a log kept of communication traffic?

□ No. Please continue to the next question.

□ Yes. What type of data is recorded in the log? (Please choose all that apply.)

□ Header

□ Payload Please describe the data that is logged.

<Please list the data elements in the log.>

8. **Can the system be accessed remotely?**

□ No.

☒ Yes. When remote access is allowed, is the access accomplished by a virtual private network (VPN)?

☒ No. Publicly accessible.

□ Yes.

9. **Is Personally Identifiable Information[2] physically transported outside of the LAN? (This can include mobile devices, flash drives, laptops, etc.)**

□ No.

☒ Yes. Personal information is transported from the publicly accessible website to both VIS and the 3rd party authentication organization.

10. **Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems[3]?**

☒ No

□ Yes. Please list:

11. **Are there regular (ie. periodic, recurring, etc.) data extractions from the system?**

☒ No.

□ Yes. Are these extractions included as part of the Certification and Accreditation[4]?

□ Yes.

□ No.

12. **Is there a Certification & Accreditation record within OCIO's FISMA tracking system?**

□ Unknown.

□ No.

☒ Yes. Please indicate the determinations for each of the following:

Confidentiality: □ Low ☒ Moderate □ High □ Undefined

[2] Personally Identifiable Information is information that can identify a person. This includes; name, address, phone number, social security number, as well as health information or a physical description.

[3] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in TAFISMA.

[4] This could include the Standard Operation Procedures (SOP) or a Memorandum of Understanding (MOU)

Integrity: □ Low ☒ Moderate □ High □ Undefined

Availability: □ Low ☒ Moderate □ High □ Undefined

PRIVACY THRESHOLD REVIEW

(To be Completed by the DHS Privacy Office)

DATE **reviewed by the DHS Privacy Office: September 20, 2010**

NAME **of** the DHS Privacy Office Reviewer: **Rebecca J. Richards**

DESIGNATION

☐ **This is NOT a Privacy Sensitive System** – the system contains no Personally Identifiable Information.

☒ **This IS a Privacy Sensitive System**

Category of System

☒ IT System

☐ National Security System

☐ Legacy System

☐ HR System

☐ Rule

☐ Other:

Determination

☐ PTA sufficient at this time

☐ Privacy compliance documentation determination in progress

☐ PIA is not required at this time

☒ A PIA is required

☐ System covered by existing PIA:

☒ A new PIA is required.

☐ A PIA Update is required.

☒ A SORN is required

☐ System covered by existing SORN:

☒ A new SORN is required.

DHS PRIVACY OFFICE COMMENTS