



**Homeland
Security**

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: April 27, 2010
Page 1 of 7

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 from the component Privacy Office, 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 DHSConnect and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.



PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

DATE submitted for review: December 1, 2010.

NAME of Project: E-Verify Program Data Collection

Name of Component: US Citizenship and Immigration Services

Name of Project Manager: Essie Bell

Email for Project Manager: essie.bell@dhs.gov

Phone number for Project Manager: 202-272-805

TYPE of Project:

Information Technology and/or System.*

A Notice of Proposed Rule Making or a Final Rule.

Form or other Information Collection.

Other: E-Verify Program Data Collection. This survey is used obtain data from employers regarding the E-Verify Program in anticipation of its increasingly widespread use.

* 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:

One of the biggest challenges for immigration reform has been development of appropriate mechanisms for reducing the likelihood that illegal immigrants will become employed in the United States by allowing employers to easily identify whether potential workers are seeking employment through use of fraudulent documents. As a result the Department of Homeland Security (DHS) and the Social Security Administration (SSA) operate E-Verify Program, a nationally available internet-based program that allows employers to electronically verify whether newly hired employees are eligible to work in the United States.

Use of E-Verify Program is voluntary in most states, but its use has become mandatory for all employers in several states, including Arizona, Mississippi, and South Carolina. In addition, several other states have enacted legislation mandating the use of E-Verify by certain *types* of employers such as public contractors, state and local government agencies, or public entities. This increased use of E-Verify together with the focus on employer verification of employment eligibility as an integral part of proposed comprehensive reform legislation makes evaluation of E-Verify's impacts through basic research critical to identifying specific areas for improvement.

USCIS is requesting the Office of Management and Budget (OMB) approval under the Paperwork Reduction Act to conduct a survey of employers in six states on the use of the E-Verify internet-based system for determining the eligibility of an individual to work in the United States. Arizona, Mississippi, and South Carolina have made use of E-Verify mandatory for all employers, exceeding Federal mandates for use of the system. Legislation is pending or has passed in 15 other states making E-Verify use mandatory for some employers. Further, there is interest in Congress in expanding mandatory use of the Program beyond current requirements for Federal contractors to include most, if not all, of the nation's employers. This research proposes to generate information about the potential impacts of mandatory E-Verify use at the state level for different industries and different size firms and to identify possible implications on both businesses and employees of a mandatory national program.

The survey requests information for a 3-year period of employers in the three mandatory states paired with three economically and demographically similar but non-mandatory "control" states: Arizona (mandatory) and Nevada (control); Mississippi (mandatory) and Alabama (control); and South Carolina (mandatory) and Tennessee (control). The information will allow comparison in patterns of E-Verify use, employment, and economic performance for each pair of states and provide insight into the impacts of state-level mandatory E-Verify use. Comparison of impacts by industry for mandatory and non-mandatory states will shed light on possible national consequences of Federally-mandated E-Verify across various industries. Employers surveyed will be representative of the mix of industries and size of firm in each state. The attached user



Privacy Threshold Analysis

Version date: April 27, 2010

Page 4 of 7

survey (Attachment E) is for use in mandatory states and the attached user survey (Attachment F) is for use in non-mandatory states.

2. Status of Project:

This is a new development effort.

This is an existing project.

Date first developed: December 1, 2010

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.

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:

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

N/A

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. Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems²?

No.

Yes.

Please list:

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

Unknown.

No.

² 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.



Privacy Threshold Analysis

Version date: April 27, 2010

Page 6 of 7

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

Confidentiality: Low Moderate High Undefined

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: January 26, 2011

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.
- PIA is required.
 - System covered by existing PIA:
 - New PIA is required.
 - PIA update is required.
- SORN not required at this time.
- SORN is required.
 - System covered by existing SORN:
 - New SORN is required.

DHS PRIVACY OFFICE COMMENTS