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 (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.

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 (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: March 19, 2010

NAME of Project: E-Verify Web Survey of Users, Designated Agents and Users of Desginated Agents

Name of Component: US Citizenship and Immigration Services

Name of Project Manager: Natasha McCann

Email for Project Manager: natasha.mccann@dhs.gov

Phone number for Project Manager: 202-272-8122

TYPE of Project:

☐ **Information Technology and/or System**[1]

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

☒ **Other: The E-Verify Program Survey of Users is a web survey and the Desingated Agents and Users of Designated Agents are telephone interviews.**

---

[1] 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:

The goal of this E-Verify Program evaluation of employers is to obtain quantitative and qualitative information about how the Program is working nationally and among a specific group of employers, to determine whether employers are using the program as intended, and to evaluate positive and negative impacts of the programs in a mandatory environment. The purpose of the linked study of DAs and UDAs is to understand how these companies work together to implement the E-Verify Program process, the burdens and advantages of using DAs, how DAs advertise for their services, how employers find DAs, and what criteria they use to hire them; the extent to which DAs and UDAs comply with the E-Verify requirements, challenges faced by DAs and their clients and how they address them, and their opinions about the desirability of a certification requirement for DAs.

The surveys will be executed by Westat, a social science research company in Rockville, Maryland, contracted to assist with the evaluation of the E-Verify Program, an Internet-based system used by participating employers to determine the employment eligibility of new hires and for some federal contractors and additional employees. Survey's of users will be Web based; interviews with DAs and UDAs will be individually conducted as semi-structured telephone interviews, which will be audio-recorded. Trained Westat project staff will conduct the telephone interviews. Westat recives a computer readable extract from Verification Information Systems (VIS), which provides a list of E-Verify users. The extract is housed in Westats secure Novel Network system. Given the semi-structured nature of the telephone interviews of DAs and UDAs and the fairly small number of respondents, the Computer Assisted Telephone Interview (CATI) methodology will not be used. The Web Users survey responses are captured and maintained in a secure survey management system, but the responses cannot be linked to individual respondents. PII is maintained separately from survey responses and linked by way of a respondent identifier (unique numerical ID). Collected data is stripped of any PII and is reported in the aggregate. Westat collects contact information for the user survey only so we can encourage respondent participation and can followup with non-respondents, and contact information is kept confidential. USCIS recieves no data that can identify a survey participant.

Data collected for the study of DAs and Users of DAs will be performed similarly to the Survey of Users. The telephone interviews will be recorded and transcripts will be made for each individual interview conducted, but Westat strips transcripts of any PII data. Again, Westat collects contact information so there can be followup with the respondents (to clarify responses, etc.). PII is maintained separately from the responses from DAs and Users of DAs through a unique numerical ID. Again, data is reported in the aggregate. All survey data collected is stored in our survey management system, which is in SqlServer 2000. The web site is secured with SSL. The database servers are firewalled from the internet zone. For analysis, user survey data will be extracted to SAS v9.2 datasets stored on Westat's secure

Novell network. The data collection system is refered to as SMS (Survey management System) that Westat designs for its surveys.

2. Status of Project:

☒ This is a new development effort.

☐ This is an existing project.

Date first developed:

Date last updated:

<Please provide a general description of the update.>

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.

In completing the survey an individual completing the form on behalf of an employer will be asked to complete contact information including Name, telephone number, title, and e-mail address. The Web Users survey responses are captured and maintained in a secure survey management system, but the responses cannot be linked to individual respondents. PII is maintained separately from survey responses and linked by way of a respondent identifier (unique numerical ID). Collected data is stripped of any PII and is reported in the aggregate. We collect contact information for the user survey only so we can encourage respondent participation and can followup with non-respondents, and contact information is kept confidential.

Data collected for the study of DAs and Users of DAs will be performed similarly to the Survey of Users. The telephone interviews will be recorded and transcripts will be made for each individual interview conducted, but we strip transcripts of any PII data. We collect contact information so we can followup with the respondents (to clarify responses, etc.). PII is maintained separately from the responses from DAs and Users of DAs through a unique numerical ID. Again, data are reported in the aggregate.

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

☐ DHS Employees

[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.

☐ Contractors working on behalf of DHS

☒ The Public

☐ The System does not contain any such information.

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?

The individual completing the survey will be asked for name, title, phone number and e-mail address along with employer information, such as name of company.

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.

☐ Yes.

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

☒ No.

☐ Yes.

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

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ 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)

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

PRIVACY THRESHOLD REVIEW

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office:

NAME of the DHS Privacy Office Reviewer: <Please enter name of reviwer.>

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