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 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
Fax: 703-235-0442

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, and fax: 703-235-0442.

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:** January 31, 2008

**NAME of Project: Customer Identity Verification Pilot**

**Name of Component: US Citizenship and Immigration Services**

**Name of Project Manager: Frank Spencer**

**Email for Project Manager: Frank.Spencer@dhs.gov**

**Phone number for Project Manger: 202-272-8951**

**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:**

The Customer Identity Verification Pilot (CIVP) is sponsored by the USCIS Transformation Program Office (TPO) to support the Agency's goal to strengthen National Security and deter/identify fraud within the USCIS benefit process through the biometric verification of it's customers. This pilot will utilize the current technology deployed by US-VISIT for customer verification and will continue to help USCIS transition towards a end-to-end electronic benefits process.

**2. Status of Project:**

☐ This is a new development effort.

☒ This an existing project.

Date first developed: October 1, 1994

Date last updated: November 1, 2007

The Automated Biometric Identification System (IDENT) is a Department of Homeland Security (DHS)-wide system for the storage and processing of biometric and limited biographic information for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions, and to provide associated testing, training, management reporting, planning and analysis, or other administrative uses.

IDENT was originally developed in 1994 as biometrics collection and processing system for the Immigration and Naturalization Service (INS). INS is now known as United States Immigration and Citizenship Services (USCIS). Today, IDENT is the primary DHS wide system for the biometric identification and verification of individuls encountered in DHS mission-related processes. IDENT is primarily a back-end system that conducts identification or verification services on behalf of numerous Government programs that collect biometric and associated biographic data as part of their mission. The mechanism to view data stored in IDENT is a Web-based interface called the Secondary Inspections Tool (SIT). USCIS will utilize IDENT to verify an individual's identity at various points in the application benefit process and will view the results of the verification through the SIT.

The SIT was originally developed for Customs and Border Protection (CBP) inspections officers to manage the US-VISIT referrals to Secondary Inspection at ports of entry. In recent years, the SIT has been adopted by users in other DHS organizations, including Immigration and Customs

Enforcement (ICE) and US Citizenship and Immigration Service (USCIS) as well as additional groups within organizations such as CBP Border Patrol.

The SIT provides you with the following capabilities:

•Conducts a 1-1 verificction of an individual's established identity.

•View determinations of certified fingerprint examiners for all potential Watchlist and Mismatch hits.

•View the details of individuals' current and previous encounters.

•Look up encounter details by a Fingerprint Identification Number (FIN), an Encounter Identification Number (EID), or an Alien Registration Number (A-Number).

•Generate reports based upon data stored in IDENT

**3. 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 see the Privacy Impact Assessment (PIA) for IDENT dated July 31, 2006 for how data is recorded in the log.

**4. Could the project relate in any way to an individual?***

☐ No. Please skip ahead to question.

☒ Yes. Please provide a general description, below.

The pilot releates to individuals as it performs one-to-one biometric identification to determine if an individual can be matched to a previously presented identity for the sam individual, to ensure that individual doesn't have any outstanding warrants/arrests and to validate whether the individual is actively on a watchlist.

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

☐ No.

☒ Yes. Why does the program collect SSNs?

The program could collect a SSN to use to search for an individual whose records are stored in IDENT. The SSN would be used as a last resort to search for a customer within the system. Travel document, A-Number would be used to search for a customer before conducting a search using the SSN. If the SSN had to be collected, a system user could ask the customer for their SSN to identify them within IDENT and verify that person's identity against the biometrics that are associated to that SSN. If an individual has an SSN that is associated to their biometric record within IDENT it will be displayed within the encounter record of that individual.

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

Other information on an individual that could be collected to search for a person within the IDENT is a Border Crossing Card (BCC), Permanent Resident Card (LPR), Passport, Reentry Permit, Refugee Travel Document, Refugee without Travel Document, Resident Alien Card, Visa (NIV or IV) and personal identifier such as a A-number, Fingerprint identification number (FIN), Encounter identification (EID) and a Social Security Number (SSN). The only information that would be retained within IDENT through the verification process would be a photograph and the person's fingerprints that are taken during the verification process. Additionally, each time a customer's identity is verified through IDENT a new encounter record

* 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.

will be generated within IDENT. An encounter record displays the date, time and the type of transaction that occurred on an individual in reference to their biometric record with IDENT. For more information please see the IDENT PIA and SORN.

**7. 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 |

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:** February 7, 2008

**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**

- ☐ PTA sufficient at this time
- ☒ A PIA is required
- ☐ National Security System
- ☐ Legacy System
- ☐ HR System

### DHS PRIVACY OFFICE COMMENTS

A PIA is required due to the collection and use of PII.