Privacy Impact Assessment
for the

United States Citizenship and Immigration Services (USCIS)

Customer Identity Verification (CIV) Pilot

August 15, 2008

Contact Point
Donald Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
(202) 272-8000

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

United States Citizenship and Immigration Services (USCIS) prepared a Privacy Impact Assessment (PIA) for the Customer Identity Verification (CIV) Pilot. The purpose of this pilot is to assess the viability of using fingerprint-based identity verification along with information from previous biometric encounters in the USCIS benefit adjudication process. USCIS will test this capability for a period of approximately four months in an operational environment consisting of four field offices. USCIS will use fingerprint scanners connected to the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program's Automated Biometric Identification System (IDENT) to implement the CIV Pilot.

Overview

Background

The Department of Homeland Security (DHS), through USCIS in part, implements United States (U.S.) immigration law and policy through the processing and adjudication of applications and petitions submitted for citizenship, asylum, and other immigration benefits. USCIS also supports national security by preventing applicants from fraudulently obtaining immigration benefits and by denying applications from individuals who pose national security or public safety threats to the U.S.

USCIS Transformation Program Office (TPO) is embarking on an enterprise-wide "transformation program" that will transition the agency from a fragmented, form-centric, and paper-based operational environment to a centralized, person-centric, consolidated environment utilizing electronic systems for thorough and accurate adjudication which will help ensure benefits are awarded to qualified applicants. The new operational environment will employ the types of online customer accounts used in the private sector. This "person-centric" model will link information related to an individual in a single account in order to facilitate applicant-friendly transactions, track activities, and reduce identity fraud. To support this effort, USCIS is deploying a series of projects that are mutually intended to demonstrate the overall benefits of the USCIS Transformation Program. One of the key projects is the Customer Identity Verification (CIV) Pilot. The CIV Pilot is a four month pilot that allows USCIS to assess the viability of using biometrics to verify that the applicant who presents for an interview is the same person who submitted fingerprints for a background check in previous stages of the adjudications process, and give USCIS adjudicators access to additional data about the applicant's previous encounters with DHS, which the adjudicator can compare to the data the applicant provided on his application.

Benefits Process

During the process of defining requirements for a new operational environment, USCIS discovered that certain steps within the application process could benefit from increased security measures to enhance national security and deter fraud more effectively. One area of concern centers on establishing and verifying the identity of persons applying for an immigration benefit. The biometric identity of a person is established the first time that person applies for a benefit. This is usually either overseas when the person applies for a visa, or at an Application Support Center (ASC) when the person is fingerprinted for background check purposes. One of the final steps in many benefits adjudication processes is an in-person interview or exam with a USCIS adjudicator. Under the existing process, USCIS does not conduct a biometric verification of the person's identity during the interview.

To create a more secure end-to-end application process, the CIV Pilot will verify an applicant's identity by comparing the biometrics of the applicant interviewing with the USCIS adjudicator with the biometrics that were previously submitted by the applicant during the benefit process or during other

encounters the individual had with DHS such as through the US-VISIT program. When an applicant presents him/herself for an interview or exam, the applicant identifies him/herself with documentation (e.g., passport). There is a risk that the person presenting for the interview is not the same person who was fingerprinted at the beginning of the benefit process because documentation can be forged or fraudulently obtained.

Typical Transaction

When a USCIS applicant arrives for the scheduled interview at a USCIS field office participating in the CIV Pilot, the applicant will be asked to provide personal identifying information, such as an Alien Registration Number (A-number), passport and issuing country, or Social Security number. The USCIS Information Officer or Adjudications Officer will type the A-number into the Secondary Inspection Tool (SIT), which provides secure remote access to the US-VISIT IDENT system. The applicant will then be asked place his index fingers on the fingerprint scanner where his fingerprints will be electronically scanned and sent to IDENT[1] for an identity match. In addition, USCIS personnel will take a digital photograph of the applicant which will be stored in IDENT. This biometric information is the same information currently collected by IDENT as part of the US-VISIT's existing process for conducting an IDENT check upon an alien's entry into the country.

To verify that the applicant at the field office is the same person who submitted biometrics to USCIS as part of the benefits application process, USCIS will use IDENT, DHS' designated biometrics repository (specifically USCIS will use an IDENT utility called the Secondary Inspections Tool [SIT]), which provides secure web-based access to IDENT). IDENT is the DHS 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. IDENT contains encounter records (including biometrics, information about the source of the encounter, and limited biographic information) originating from multiple DHS components, plus Department of State (DOS), Department of Justice (DOJ) Federal Bureau of Investigations (FBI), Interpol, Department of Defense (DOD), and state and local law enforcement organizations.

Once the identity of the applicant is verified, USCIS will be able to retrieve a list of encounters DHS has had with that applicant based on his or her biometrics. These additional encounters include the circumstances surrounding each previous time the applicant's biometrics were enrolled in the DHS IDENT system, which may include the applicant's application for a visa to enter the U.S., entries into and exits from the U.S., and whether the person is of interest to the U.S. or international law enforcement and/or intelligence agencies because of suspected or confirmed illegal activity. The list of encounters along with the associated information will be printed and will be placed in the applicant's Alien file (A-file) or temporary A-file (T-file). The adjudications officer will then use these files during the interview process. Encounter information printed and viewed by the adjudications officer includes but is not limited to the following: date and time of previous encounter; type of encounter (i.e. entry, exit, visa issuance); name given at the time of the encounter; and the subject's picture. The encounter information, which is displayed and printed, does not include the fingerprint images.

The adjudicator may use this additional information to make a determination of whether the applicant is eligible for the benefit sought. Of particular interest to an adjudications officer is the name given at the time of the previous encounter and the date, time, and type of the previous encounter. This information can be used to clarify and substantiate claims made by the applicant, but may also be used to find areas where material facts have been misrepresented. To ensure that the information provided by IDENT to the USCIS adjudicator is not misunderstood, adjudications officers will go through a training program that explains the meaning and importance of the information displayed. In addition, all derogatory watch list encounter information, which is displayed, includes a set of specific instructions that

[1] For additional details about the IDENT system, see the July 31, 2006 US-VISIT IDENT PIA at dhs.gov/privacy.

typically directs an officer to a person or organization for additional information or instructions. In the majority of cases (depending on the specific instructions associated with the watch list hit), the watch list information will also be printed and will become part of the applicant's A-file.

This PIA covers the deployment of the CIV Pilot for its four-month assessment period and will be supplemented accordingly as additional USCIS applications and system functionalities are added to the CIV Pilot. The CIV Pilot will initially be deployed, but may not be limited to, the following four USCIS District Field Offices:

- Portland, Maine
- El Paso, Texas
- San Francisco, California
- Jacksonville, Florida

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

During the CIV Pilot, USCIS will ask the applicant to show his or her identification or travel document, such as a Border Crossing Card, Permanent Resident Card, Passport, Reentry Permit, Refugee Travel Document, Resident Alien Card or Visa. Based on the information provided by the card, USCIS will use the A-number, passport number and issuing country, or Social Security number to retrieve the person's record in IDENT, and to initiate the identity verification. USCIS personnel will also be able to retrieve an applicant's record in IDENT using the following internal system identifiers: Fingerprint Identification Number (FIN), Encounter Identification (EID), or Enumerator.

Once the applicant's identifier has been entered into IDENT to initiate the identity verification, USCIS will collect an applicant's digital photo and index fingerprints along with an identifier (usually the A-number or passport number and country of issuance) and enter that information directly into IDENT. USCIS will not keep a separate copy of this information. If IDENT verifies that the person's fingerprints match those on file for the identifier, the verification will result in an encounter record in IDENT. The encounter created will contain the person's photo, fingerprints, the date and time of the encounter, and a label indicating that the encounter occurred at a USCIS field office.

When USCIS personnel participating in the CIV Pilot enter an applicant's identifier into SIT, information from previous encounters stored in IDENT are displayed. IDENT encounter history is then displayed within the SIT. Among others, IDENT will provide details on the following types of previous encounters: entry, exit, lookout, recidivist, visa application, Border Crossing Card application, USCIS application, Asylum, one-to-one verification, CBP or ICE apprehension, special alien registration (SAR), CBP Global Enrollment System (GES), TSA Alien flight school Program (AFSP), and TSA Airport Workers (AW). As part of the CIV Pilot, USCIS will print the previous encounter history out in hard copy form and file it in the applicant's A-file.

1.2 What are the sources of the information in the system?

The information displayed to adjudicators through the CIV Pilot IDENT data. IDENT data is collected from federal, state and local organizations that have law enforcement or immigration functions. From inside DHS, data may have been collected from individuals by such agencies as ICE, CBP, USCIS, Transportation Security Administration (TSA), United States Coast Guard (USCG), or another DHS agency in support of a DHS mission. From outside of DHS, data is collected by external organizations such as the Department of State, Department of Justice Federal Bureau of Investigations, Department of Defense, and other governmental organizations that collaborate with DHS in pursing DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

1.3 Why is the information being collected, used, disseminated, or maintained?

USCIS uses the digital fingerprints, digital photograph, and limited biometric information collected for the purpose of verifying an applicant's identity at various points throughout the application benefit process. Previous IDENT encounter data is used to identify whether the applicant may have misrepresented facts on his or her application. Identity verification is done in an effort to deter fraud and enhance national security, to deliver the right benefit to the appropriate applicant at the right time, and to ensure that inappropriate applicants do not receive benefits to which they are not entitled. Adjudicators use previous encounter data to see if potentially false identities were used by the applicant in prior encounters, and also to verify the date and time and type of encounter against what the applicant has reported to USCIS. For example, the applicant may report to USCIS that he has not left the country for a period of time, but IDENT encounter data may reveal that the applicant entered the country from abroad during that same period of time. This information can be used to clarify or substantiate claims by the applicant, but may also be used to find areas where facts have been misrepresented.

The applicant's fingerprints and photograph are used, collected and maintained in IDENT through the verification process. Additionally, limited biographic data will need to be collected and used in the biometric the verification process.

1.4 How is the information collected?

Information will be collected directly from the applicant seeking a benefit. The applicant will present a specific document or personal identifier depending on the desired benefit, to the USCIS employee or contractor who will locate that applicant within IDENT. The USCIS employee or contractor, who is authorized to use IDENT and has appropriate access, will then collect fingerprints and a facial photograph using a fingerprint scanner and web camera.

Previous encounter data is collected from IDENT when the person's identifier (e.g., A-number) and fingerprints are verified by IDENT.

1.5 How will the information be checked for accuracy?

The IDENT interface to the fingerprint scanner used by USCIS in the CIV Pilot has the ability to tell if a fingerprint is of unacceptably low quality. If an applicant's prints are unacceptable, the interface prompts the USCIS user to capture the applicant's prints again. The identity management process employed by IDENT is extremely accurate. Additionally, IDENT sends all potential mismatch and Watch list hits to a certified fingerprint examiner where a final "match" or "no match" status on the applicant's fingerprints is rendered. However there are rare occasions where the quality of the fingerprint is so poor that even a

fingerprint examiner may not be able to confirm a match or mismatch. In these cases, the system will return a response of "unverifiable" and the interview must proceed without a biometric identity confirmation or previous encounter data.

This quality assurance process ensures that the person presenting for the interview is the same as the person previously encountered by DHS, and that all previous encounters match the same individual.

Encounter data received from IDENT will include biographic data. If the biographic data within the encounter data differs from the biographic data the adjudicator has on file, the adjudicator, at his discretion (based on training and professional experience) may process the application, resolve the discrepancies with the applicant, or refer the file to USCIS staff to investigate fraud and national security concerns. Regardless of the outcome the adjudication process, the IDENT record will be updated to include the fact that DHS, through USCIS, encountered the applicant as part of the benefit application process.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The CIV Pilot is given authority to collect this information by the following:

- The Immigration and Nationality Act, 8 U.S.C. Section 1101(b) (1) (F) and 8 C.F.R. Section 204.3
- Intelligence Reform and Terrorism Prevention Act of 2004, Pub.L. No. 108-458, Title VII, Section 7208, dated December 17, 2004
- Executive Order 13356, Strengthening the Sharing of Terrorism Information to Protect Americans, dated August 27, 2004
- Homeland Security Presidential Directive-11 (HSPD-11), *Terrorist-Related Screening Procedures*, dated August 27, 2004

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The primary risk of using the IDENT is unauthorized access to or disclosure of information contained and maintained within IDENT. To mitigate this risk, a number of business and system rules have been implemented. Access to IDENT is given only to a limited number of government and contractor users who need it to perform their official duties. Access to various features of IDENT is governed by logical access controls. All authorized users must authenticate using a user ID and password. Lastly, through policies and procedures, DHS limits the use and access of all data in IDENT to the purposes for which it was originally collected.

The risk of collecting inaccurate or outdated data is mitigated by the fact that USCIS collects biometric and limited biographic information directly from an applicant. The CIV Pilot provides users with the ability to perform full queries on applicants and data stored within IDENT. With this function, there is a risk that users will search for information on individuals and topics beyond the scope of their work. This risk is mitigated by IDENT training, supervisory oversight, and enforcement of DHS policies that limit the use and access of all data in IDENT to the purposes for which it was collected. An audit trail will be kept for system access and all transactions that request, create, update, or delete information from the system. The audit trail, which includes the date, time, and user for each transaction, will be secured from unauthorized modification, access, or destruction, kept for at least 90 days, and routinely audited.

There is a risk that once previous encounter data is printed out, it may be lost or misfiled. This risk is mitigated by the fact that the applicant's A-file is at the same field office as the adjudicator conducting the interview, so the printout will be filed into the A-file consistent with the office's existing process for properly filing all interview materials. In the event that USCIS has a hard copy record that belongs in the A-file but the A-file is in another location, that office will create a temporary file (T-file) that is tracked until it is reunited with the permanent A-file, so that loose documents are not lost.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

For the purposes of this pilot USCIS will typically use the A-number to direct the IDENT system to the correct set of biometrics for one-to-one verification. Once the identity is verified, the information contained in IDENT's prior biometric encounters will be used in the adjudication process to substantiate a applicant's claims, or to identify areas where material facts have been misrepresented.

2.2 What types of tools are used to analyze data and what type of data may be produced?

USCIS will not use any tools to analyze data through the CIV Pilot. However, USCIS will use IDENT to verify that the applicant's fingerprints submitted at the time of the interview match any fingerprints previously submitted by that applicant earlier in the benefits process. The type of data that IDENT will produce for USCIS in performing this identity verification is whether the verification was successful, or if the verification was not successful ("pending mismatch"), in which case an experienced fingerprint examiner working for the IDENT system will review the fingerprint and make a determination.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above- described uses.

Given the amount and complexity of previous encounter data available to USCIS through the CIV Pilot, there is a risk that the adjudicator may misinterpret the data. To ensure that the information returned to USCIS personnel by IDENT is not misunderstood, adjudications officers will go through a training program that explains the meaning and importance of the information displayed. In addition, all derogatory watch list encounter information, which is displayed, includes a set of specific instructions that typically directs an officer to a person or organization for additional information or instructions.

Access to IDENT is given only to a limited number of government and contractor users who need it to perform their official duties. Access to various features of IDENT is governed by logical access controls that prevent, limit, and detect access to the network, systems, and information. All authorized users must authenticate using a user ID and password. Lastly, through policies and procedures, DHS limits the use and access of all data in IDENT to the purposes for which it was collected.

IDENT data is analyzed as part of the PIA process to ensure that it supports one or more DHS missions. The PIA and/or data sharing agreements define the controls that are in place to ensure that data is used in accordance with the routine uses. The data owners are ultimately responsible for ensuring that the data is used appropriately. This is done by the establishment of data sharing agreements that stipulate prescribed and permitted activities and uses, auditing requirements, and integrity controls.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

USCIS will collect applicants' A-number or other biographic identifier, fingerprints, and digital facial photograph. This data will be retained as an encounter in IDENT. USCIS will not retain this newly captured data. A hard copy print of the applicant's previous IDENT encounters, including date and time of previous encounter; type of encounter (i.e. entry, exit, visa issuance); name given at the time of the encounter; and the subject's picture are retained by USCIS in the applicant's A-file. The encounter information does not include the fingerprint images.

3.2 How long is information retained?

In accordance with the IDENT retention schedule, records in IDENT will be retained until the statute of limitations has expired for all criminal violations or until the records are older than 75 years.

Previous encounter information maintained in the A-file will be retained in accordance with the A-file retention schedule, which is for 75 years from the date the file is retired to the Federal Records Center or date of last action (whichever is earlier) and then destroyed.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention schedule for IDENT and the A-file have been approved by NARA.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

In accordance with the System of Record Notice (SORN), the retention period for data displayed within IDENT is 75 years because the information in the database may be used to enforce immigration law and consequently needs to be available for the length of time of the potential statutes of limitations for violations of the immigration code. To ensure compliance with existing regulatory policies and guidance, IDENT is mandated to store and retain potential immigration cases information for 75 years in support of enforcement procedures.
Previous encounter information will be used in the adjudicative process and will be printed and stored in the applicant's A-file. The A-Files are retained to support adjudication decisions, law enforcement uses, and protection of national security. Additionally, via an approved disposition and retention schedule, NARA has directed that the information be retained for a specified period. The information is retained for the specified period because the relationship between USCIS and the applicant may span an applicant's lifetime.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

IDENT data may be shared with other DHS components, with the consent of US-VISIT, 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 use that requires the use of biometrics to identify or verify the identity of individuals.

Previous encounters filed into the A-file are shared, along with the entire A-file with Customs and Border Protection (CBP), which performs the border and inspection processes; and Immigrations and Customs Enforcement (ICE), which performs the investigatory, deportation, and immigration court functions. Although USCIS is the custodian of the A-File, all three components (USCIS, CBP, ICE) create and use A-Files. Information contained within the A-File may also be shared with other components within DHS responsible for law enforcement activities and protection of national security, specifically, TSA and USCG.

4.2 How is the information transmitted or disclosed?

In most cases the data is transmitted between IDENT and other systems on the DHS core network, an unclassified, secured wide area network. Information may be shared electronically via secure internal or external network connection or through the following modes:

- Direct limited access to IDENT where personnel of organizations are co-located with DHS personnel with access to the system
- Limited direct connections to other systems where only data that is relevant and necessary to the other agencies (routine users) mission may be transmitted directly between IDENT and

those other systems; i.e., ENFORCE, SBI Federated Query, IAFIS, SEVIS, CLAIMS, ADIS, and RAPS. Data will be shared with the consent of the data owner for DHS national security, law enforcement, immigration, intelligence, and other DHS mission related functions, and to provide associated testing, training, management reporting, and other administrative uses that require the use of biometrics to identify or verify the identify of individuals.

- Secure transfer, including encryption, on portable media when there is no direct connection between systems.

The mode of transmission or disclosure will be described for each program in the PIA or MOU or other data-sharing agreement associated with that particular program.

A-files are hardcopy files that are transferred to the DHS component in need of the file in hardcopy format. Under a new initiative, USCIS is digitizing the information in some A-files under the Integrated Digitization Document Management Program (IDDMP). Digitized data transmitted within IDDMP (from scanning to the repository to users of the information in the system) on the DHS core network, an unclassified, secured wide area network.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

In many cases DHS internal data sharing is required to comply with statutory requirements for national security and law enforcement. In all cases, however, this data must be kept secure, accurate, and appropriately controlled. Data users ensure that any privacy risks are mitigated through data sharing agreements that require auditing, access controls, re-sharing limits, and other physical, technical, and administrative controls.

The CIV Pilot will provide additional information to the adjudicator from IDENT, create a new encounter record about the interview in IDENT, and provide a list of previous encounters to be included in the A-file. Any further sharing of that data will occur in compliance with the existing IDENT and A-file processes and data sharing agreements.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS, which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

USCIS will not share any information external to DHS through the CIV Pilot. However, DHS does share information externally via IDENT and the A-file pursuant to routine uses set forth in those systems' existing SORNs. Under the CIV Pilot, IDENT will record the applicant's biometric verification encounter at USCIS. When IDENT returns to USCIS the applicant's previous encounters, USCIS will print that information and file that information into the A-file.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

All external sharing by DHS via IDENT and the A-file will be subject to applicable laws, regulation, and memoranda of understanding, business rules and any other appropriate restraints on external data sharing as described by the systems' respective SORNs: Alien File (A-File) and Central Index System (CIS) DHS-USCIS-001, January 16, 2007, 72 FR 1755, and DHS Automated Biometric Identification System (IDENT) DHS/USVISIT-0012, June 5, 2007, 72 FR 31080.

For example, external agencies, such as DOS, would be able to view each encounter USCIS had with an applicant through the IDENT.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information may be shared electronically via secure internal or external network connection or through the following modes:

- Direct limited access to IDENT where personnel of organizations of ICE Investigations, CBP Border Patrol, CBP OFO, USCIS Asylum, USCIS Refugee Affairs, Coast Guard, US-VISIT, Detention & Removals, USCIS Application Support Centers that are co-located with DHS personnel with access to the system
- Limited direct connections to other systems where only data that is relevant and necessary to the other agencies (routine users) mission may be transmitted directly between IDENT and those other systems. Data will be shared with the consent of the data owner for DHS national security, law enforcement, immigration, intelligence, and other DHS mission related functions, and to provide associated testing, training, management reporting, and other administrative uses that require the use of biometrics to identify or verify the identify of individuals.
- Secure transfer, including encryption, on portable media when there is no direct connection between systems.

The specific mode of transmission or disclosure for each program will be described in an MOU or other data sharing agreement associated with that particular program.

The sharing of information will be controlled by the underlying PIA for the entities' collection activity, as well as any executed Memorandum of Understanding or other data sharing agreement between the parties. This includes controls such as passwords, certificates for key management, physical access rosters, usage/access reports that limit the use of data uniquely identifying an individual within the DHS management environment only.

The A-file may be shared with external organizations pursuant to its SORN. For example, USCIS may allow a federal law enforcement officer to view the A-file on USCIS premises as part of the officer's law enforcement investigation.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The CIV Pilot will not involve data sharing external to DHS. Information collected under the CIV Pilot will be stored in IDENT or in the A-file, and information will be shared from those systems according to their existing processes and data sharing agreements.

Outside the scope of the CIV Pilot, external data sharing of IDENT information is required to comply with statutory requirements for national security and law enforcement. In all cases, however, this data must be kept secure, accurate, and appropriately controlled. Data users ensure that any privacy risks are mitigated through data sharing agreements that require auditing, access controls, re-sharing limits, and other physical, technical, and administrative controls.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

This PIA notice will be published on the DHS website prior to the launch of the Customer Identity Verification Pilot.

Additionally, within the instructions of each benefit form there is a 'Privacy Act Notice' section detailing authority and uses of information. The incorporated statement is as follows: "*We ask for the information on this form, and associated evidence, to determine if you have established eligibility for the immigration benefit for which you are filing. Our legal right to ask for this information can be found in the Immigration and Nationality Act, as amended. We may provide this information to other government agencies. Failure to provide this information and any requested evidence may delay a final decision or result in denial of your Form #-### (Form number of particular benefit)*" The application also contains a signature certification and authorization to release any information from an applicant record that USCIS needs to determine eligibility, including biometric and biographic information.

Notice of information collection is also provided by the following SORNs: Alien File (A-File) and Central Index System (CIS) DHS-USCIS-001, January 16, 2007, 72 FR 1755, and DHS Automated Biometric Identification System (IDENT) DHS/USVISIT-0012, June 5, 2007, 72 FR 31080.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals who submit applications to USCIS will be presented with a Privacy Act Statement and a signature release authorization on each application related to benefit. The Privacy Act Statement details the authority and uses for information that the individual provides on the application. Each application also contains a signature certification and authorization to release any information from an applicant's record that USCIS needs to determine eligibility. It is within the rights of the individual to decline to provide the required information; however, it will result in the denial of the applicant's benefit request.

On its application forms, USCIS requires certain biographic information and may also require submission of fingerprints and photographs. This information is critical in making an informed adjudication decision in granting or denying a USCIS benefit. The failure to submit such information would prohibit USCIS from processing and properly adjudicating the application and thus preclude the applicant from receiving the benefit. Therefore, through the application process, applicants have consented to the use of the information for adjudication purposes, including background investigations.

The applicant may be unable to submit fingerprints of a high enough quality to be verified using IDENT. If an applicant's prints are unacceptable, the system will return a response of "unverifiable" and the interview must proceed without a biometric identity confirmation.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

A Privacy Act statement detailing authority and uses of information is presented to the applicant. The application also contains a signature certification and authorization to release any information from an applicant record that USCIS needs to determine eligibility, including biometric and biographic information.

All USCIS applications include a Privacy Act Statement and a signature release authorizing "…the release of any information from my records that USCIS needs to determine eligibility for the benefit…"

When the applicant signs the application, consent is given for any use to determine eligibility.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The collection of personally identifiable information is a required part of the adjudication process, which must occur prior to the granting of an immigration benefit. Under the CIV Project, the applicant submits his or her information directly to USCIS, so he or she is aware of information collection at that time. All collected information can be used for adjudicating benefit applications, conducting background checks and other purposes USCIS deems appropriate (e.g., law enforcement investigations and national security issues). The privacy risk that an applicant may not be fully aware that their information will be used to conduct a background investigation is associated with this particular collection of information. In order to mitigate this risk, USCIS provides a Privacy Act statement on its applications. The application also contains a signature certification and authorization to release any information provided by the applicant. To further mitigate this risk, USCIS is issuing this PIA for the Customer Identity Verification Pilot.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

In order to gain access to one's information collected by USCIS, a request for access must be made in writing and addressed to the Freedom of Information Act/Privacy Act (FOIA/PA) officer at USCIS. Individuals who are seeking information pertaining to them are directed to clearly mark the envelope and letter "Privacy Act Request." Within the text of the request, the subject of the record must provide his/her account number and/or the full name, date and place of birth, and notarized signature, and any other information which may assist in identifying and locating the record, and a return address. For convenience, individuals may obtain Form G-639, FOIA/PA Request, from the nearest DHS office and used to submit a request for access. The procedures for making a request for access to one's records can also be found on the USCIS web site, located at www.uscis.gov.

An individual who would like to file a FOIA/PA request to view their USCIS record may do so by sending the request to the following address:

U.S. Citizenship and Immigration Services

National Records Center

FOIA/PA Office

P.O. Box 648010

Lee's Summit, MO 64064-8010

Freedom of Information Act requests may also be submitted to this address.

To request access to data in IDENT, write to:

US-VISIT Privacy Officer

US-VISIT Program

U.S. Department of Homeland Security

245 Murray Lane, SW

Washington, DC 20528

USA

Certain information may be exempt from disclosure pursuant to the Freedom of Information Act/Privacy Act, because displaying the data in IDENT could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, and reveal investigative interest on the part of DHS or another agency. Access to records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Applicants have an opportunity to correct their data during interviews. Otherwise they may submit a redress request directly to the USCIS Privacy Officer who refers the redress request to USCIS' Office of Field Operations, Office of International Operations or to the US-VISIT Program, as applicable. If an applicant believes their file is incorrect but does not know which information is erroneous, the applicant may file a Privacy Act request as detailed in Section 7.1. Redress procedures for IDENT are established and operated by DHS through Traveler Redress Inquiry Program (DHS TRIP) which can be accessed at www.dhs.gov/trip.

7.3 How are individuals notified of the procedures for correcting their information?

Applicants are notified of the procedures for correcting their information on USCIS application instructions, the USCIS website at www.uscis.gov, by USCIS personnel who interact with them and through publication of this PIA.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Formal redress procedures are described in section 7.2 above.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Redress procedures are established and operated by the program through which the data are collected. Additionally, correction and redress rights are provided as set forth in Sections 7.1 through 7.4 above.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

DHS personnel and contractors who have received the appropriate security and privacy training will have access to IDENT. All users must complete the appropriate access form (e.g., Form G-872B) to record authorization of access. The primary user groups at USCIS include: adjudication officers, adjudication supervisors and adjudication support staff. Basic access will be granted to all authorized users, while additional access will be determined on a case-by-case basis by US-VISIT, limited to the extent required for the particular user group to complete their responsibilities.

8.2 Will Department contractors have access to the system?

IDENT may be used by contractors to verify an applicant's identity at any point in time during the benefit application process. All access to IDENT follows the logical access controls set up for access to US-VISIT computer systems. Access controls are applied to contractors and federal employees equally. IDENT has a robust set of access controls including role based access, and interfaces which limit individuals' access to the appropriate discrete data collections to which they should have access.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All DHS system users complete mandatory annual computer security awareness and privacy training which addresses computer usage and privacy issues. Users will also complete IDENT training class which will reiterate privacy and security issues as well as teach the users how to use the system.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The data is secured in accordance with DHS and Federal security requirements, including the FISMA requirements. SIT is a subsystem of IDENT. IDENT was re-certified and accredited on May 14, 2007, expiring on May 14, 2010.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

IDENT secures its data by complying with the requirements of DHS information technology security policy, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). This handbook established a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules. IDENT is periodically evaluated to ensure that it complies with these security requirements.

Security controls are in place to insure that information maintained within IDENT is used by staff that has been authorized. IDENT has a robust set of access controls including role based access, and interfaces which limit individuals' access to the appropriate discrete data collections to which they should have access. Misuse of data is prevented or mitigated by requiring that users conform to appropriate security and privacy policies, follow established rules of behavior, and be adequately trained regarding the security of their systems. Also, periodic assessments of physical, technical, and administrative controls are performed to enhance accountability and data integrity. External connections must be documented and approved with both parties' signatures in an Interconnection Service Agreement (ISA), which outlines controls in place to protect the confidentiality, integrity, and availability of information being share or processed.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

DHS has a robust security program that employs physical, technical and administrative controls. These controls are validated through a Certification and Accreditation process as specified within DHS policies and procedures. Additionally, IDENT maintains activity logs including transactions by users. Reports will be produced to verify that user's activity is consistent with their permissions. All individuals who use IDENT will be tracked through the IDENT audit log. Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users will be broken into specific classes with specific access rights. Audit trails will be kept in order to track and identify any unauthorized use of system information. Data encryption will be employed at every appropriate step to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Further, IDENT complies with DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack, and unauthorized information dissemination.

Additionally, all USCIS employees are required to attend annual privacy training and security awareness training, which covers the handling of personally identifiable information and how to use IT systems appropriately and securely.

Users have limited access that is established based on their role. US-VISIT on a case-by-case basis will determine the level of access a user has. There are only two roles within SIT:

- General Access – Users can search and view records and perform 1:1 verification
- Advanced Access – Users can do anything a General Access user can and additionally they can run reports and view fingerprint images

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The CIV Pilot is a four month pilot that allows USCIS to assess the viability of using IDENT at four USCIS field offices. USCIS will use this access to IDENT for two purposes: (1) to use biometrics to verify that the applicant who presents for an interview is the same person who submitted fingerprints for a background check in previous stages of the adjudications process, and (2) to give adjudicators access to the applicant's previous encounter data in IDENT, which the adjudicator can compare to the data the applicant provided on his application.

9.2 What stage of development is the system in and what project development lifecycle was used?

The CIV Pilot is in the pilot phase. Upon conclusion of the pilot phase, USCIS will gather the results of the pilot to determine whether the CIV Pilot as designed is beneficial to the adjudicators at USCIS field

offices, whether additional improvements need to be tested, and whether to implement the solution to additional USCIS offices.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

USCIS will remotely access IDENT during the CIV Pilot. This use involves remotely transmitting the USCIS applicant's digital fingerprints and photograph to IDENT, which is a DHS-wide repository for biometrics and associated limited biographic data. Under the CIV Pilot, USCIS use of IDENT is limited to two purposes. First, USCIS will use IDENT to perform identity verification of the applicant to confirm that USCIS is interviewing the same person who submitted fingerprints earlier in the application process. Second, USCIS will use previous encounter data accessible via IDENT to provide adjudicators with the applicant's previous encounters in IDENT, which provides the adjudicator with additional information that may support or contradict the information provided to the adjudicator by the applicant.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security