Privacy Impact Assessment
for the

Automated Biometric Identification System (IDENT)

July 31, 2006

Contact Point
Steve Yonkers, Privacy Officer
US-VISIT Program Office, DHS
(202) 298-5200

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

This privacy impact assessment (PIA) for the Automated Biometric Identification System (IDENT) describes changes to IDENT corresponding to the publication of a new IDENT system of records notice (SORN). IDENT is a Department of Homeland Security (DHS)-wide system for the collection 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.

Introduction

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 a biometrics collection and processing system for the Immigration and Naturalization Service (INS). Since that time, the INS, as well as numerous other organizations, were subsumed and reorganized into DHS. This change has meant that the intended use of IDENT has expanded beyond that for which it was initially designed. This has necessitated a revision to the system of records notice (SORN). Today, IDENT is the primary DHS-wide system for the biometric identification and verification of individuals 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. These Government programs are essentially "users" of IDENT biometric identification and verification services. This privacy impact assessment (PIA) will focus specifically on IDENT. Each of the interconnected Government programs will be responsible for creating a PIA for their programs, and explaining the use of IDENT in relation to their mission.

Section 1.0
Information collected and maintained

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

1.1 What information is to be collected?

IDENT collects biometric, biographic, encounter related data, for operations/production, testing, and training environments. Biometric data includes but is not limited to fingerprints and photographs. Biographical data includes but is not limited to name, date of birth, nationality, and other personal descriptive data. The encounter data provides the context of the interaction with an individual including but not limited to location, document numbers, and/or reason information collected. Test data may be real or simulated biometric, biographic, or encounter related data.

1.2 From whom is information collected?

Data is collected by various programs and then transmitted to IDENT. Data may be transmitted on a real-time basis from DHS internal or external interconnected systems, or data could be transmitted on a single-time ad hoc basis. From within DHS, data may have been collected from individuals by such agencies as Immigrations and Customs Enforcement (ICE), Customs and Border Protection (CBP), United States Citizenship and Immigration Services (USCIS), Transportation Security Administration (TSA), United States Coast Guard (USCG), or any other DHS agency in support of a DHS mission. From outside of DHS, data is collected from such external organizations as Department of State (DOS), Department of Justice (DOJ) Federal Bureau of Investigations (FBI), and Department of Defense (DOD) and other governmental organizations that collaborate with DHS in pursuing DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions. Data collections will be described in the respective program's PIA associated with the specific data collection.

1.3 Why is the information being collected?

Biometric and limited biographic data is being transmitted to and stored in IDENT to support DHS mission activities that require biometric identification and verification. In most cases, biometric data will have multiple uses, (e.g., fingerprint data may be initially collected from a visa applicant by DOS and transmitted to IDENT for identification and watchlist checks and then collected by CBP from the same individual at the time the person applies for admission and transmitted to IDENT for identity verification against the visa record and updated watchlist checks). Storing biometric data in one system and then allowing for multiple uses minimizes duplication of collection, storage, and processing of identical data. It enhances both DHS' ability to identify those who present threats and facilitate those who DHS has encountered and checked before. Furthermore, having a single biometric matching system for multiple purposes allows for the development of specialized systems as well as experienced operators.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

The data maintained in IDENT is collected based on the authority for the programs that collected the data from the individuals. These authorities are described in the PIAs, SORNs, or other materials for each of these programs.[1]

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

As a primary system for the storage and processing of biometric data used for various DHS mission-supporting activities, IDENT deals with many organizational data collection needs. Each new collection is reviewed to ensure that the data types are appropriate for IDENT and that the storage and/or processing requested from IDENT is being made to support a DHS mission. Risks associated with specific data collections will be described in the appropriate associated program PIA.

The aggregation of data from these numerous programs creates a potential risk to privacy for two reasons. One, the aggregated collection may be a more valuable and attractive target and two, simply aggregating data can, in some cases, result in information that exceeds the specific purposes the separate data elements were collected for in the first place. With regard to the security of the aggregated data in IDENT, it is more efficient and cost-effective to protect one data system through a rigorous security program employing physical, technical, and administrative controls, as described in Section 8 below, than if the data were contained in separate systems, in different locations, but that all must still link together to provide DHS' required functionality.

With regard to the concern over data aggregation itself, DHS limits the use and access of all data in IDENT to the purposes for which it was collected.

Section 2.0
Uses of the system and the information

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

---

[1] See for example, 69 FR 2608-2615, United States Visitor and Immigrant Status Indicator Technology (US-VISIT) PIA, 16 January 2004.

2.1 Describe all the uses of information.

The data in IDENT is used by DHS 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 that require the use of biometrics to identify or verify the identity of individuals. These purposes relate to administering or enforcing the law, national security, immigration, intelligence, or other DHS-mission related function. Specific uses are described in PIAs associated with programs that use the information.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

IDENT is a biometric matching system, DHS does not conduct data mining within IDENT. However, the data provided from IDENT to a particular program or linked to an IDENT record may be used in data mining by that program. Any use of the data in this manner must be approved by the data owner and would be described in the PIA associated with the particular program.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Much of the functionality of IDENT relies on its ability to match encounters either one to one (i.e., is this the same person we previously encountered with this identity?) or one to many (i.e., have we ever encountered this person before?). This means that great value is placed on the accuracy, quality, and completeness of the information collected and transmitted to IDENT. However, because of the diverse environments in which this data is collected, accuracy, completeness, and quality may vary considerably. Although IDENT performs certain quality checks (e.g., determining the quality of a fingerprint captured and its suitability for matching in the future) and seeks to ensure that the data meets a minimum level of quality and completeness, it is ultimately the responsibility of the data owner, whether an organization external or internal to DHS, to ensure the accuracy, completeness, and quality of the data.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above-described uses.

As part of the standard processing of data, all data in IDENT is checked for a minimum level of quality and completeness. All new uses of IDENT data are analyzed as part of the PIA process or in the development of data sharing agreements, as applicable, to ensure that they support one or more DHS missions. The PIA and/or data sharing agreements define the controls that will be in place to ensure that data is used in accordance with the allowed uses. For example, all IDENT user access account holders must complete the password issuance control process in order to receive account logins and passwords. 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 proscribed 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 is the retention period for the data in the system?

Records will be retained until the statute of limitations has expired for all criminal violations or that are older than 75 years.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes, the retention schedule has been approved.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

As an INS legacy system, the retention period for IDENT was established when the system was used primarily for holding the biometrics of subjects of interest in immigration and border management or law enforcement activities. However, now, as a DHS-wide repository of

biometrics for any of its missions, IDENT holds data that may not need to be held for 75 years. Consequently, DHS is currently undertaking a reevaluation of the retention policy, especially in light of the aggregation of data not previously combined, and may determine a new retention period or combination of retention periods dependent upon the data collected.

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 organizations is the information shared?

As a primary DHS-wide repository of biometrics, IDENT data is shared throughout DHS. Components with whom IDENT data is shared are usually responsible for preparing a PIA which describes the specifics of that sharing.

4.2 For each organization, what information is shared and for what purpose?

IDENT shares any of the data contained in IDENT, 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, planning and analysis, or other administrative uses that require the use of biometrics to identify or verify the identity of individuals.

4.3 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. Other types of transmission or disclosure may be required in some circumstances. 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.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

In many cases DHS internal data sharing is required to comply with statutory requirement for national security and law enforcement. In all cases however, this data must be kept secure,

accurate, and appropriately controlled. Data owners ensure that any privacy risks are mitigated through data sharing agreements that require such things as auditing, access controls, re-sharing limits, and other physical, technical, and administrative controls.

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 organizations is the information shared?

IDENT shares data with Federal, state, local, tribal, foreign or international government agencies charged with DHS national security, law enforcement, immigration, intelligence, or other DHS mission-related functions.

5.2 What information is shared and for what purpose?

IDENT may share any of the data contained in IDENT, 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, planning and analysis, other administrative uses that require the use of biometrics to identify or verify the identity of individuals.

5.3 How is the information transmitted or disclosed?

Information is transmitted or disclosed to external organizations in one of three ways:

- Direct limited access to IDENT where personnel of these organizations are co-located with DHS personnel with access to the system;
- Limited direct connections to other systems where data may be transmitted directly between IDENT and those other systems; and
- Data is securely transferred on portable media when there is no direct connection between systems.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

DHS has entered into MOUs or other agreements with non-DHS organizations with which IDENT shares information. These agreements provide the conditions of sharing or disclosure, including governing the protection and use of the information.

5.5 How is the shared information secured by the recipient?

External connections must be documented and approved with each party's signature in an interagency security agreement (ISA) that outline controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Organizations with which IDENT shares information must agree to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information. Furthermore, recipient organizations must notify DHS as soon as reasonably practicable, but not later than within 24 hours, after they become aware of any breach of security of interconnected systems or unauthorized use or disclosure of personal information.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

All information users must participate in a security and privacy training program. Consultants and contractors must also sign a non-disclosure agreement.

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

Data shared with external organizations must be kept secure, accurate, and appropriately controlled. Data owners ensure that any privacy risks are mitigated through data sharing agreements that require such things as 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? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The extent of notice will vary depending on the particular collection. In most cases, notice is provided by means of a PIA published on the DHS website and in the Federal Register by the specific program or organization conducting the collection. Certain national security and law enforcement collections may not provide advance notice, or may not provide notice through a PIA because to do so would jeopardize the ability to collect the information in the first place. Notice surrounding the changes to IDENT necessitating this PIA is also provided by a revision to the SORN.

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

The opportunity and/or right of an individual to decline to provide their data will depend on the purpose of the collection which, if such an opportunity or right exists, will be described in the PIA specific to the collection. However, in most cases, because of the DHS national security, law enforcement, immigration, intelligence, or other DHS-mission related purposes for which the information is collected, such opportunities to decline may be limited (eg., your recourse may be to not apply for a visa in the BioVisa context or to not apply for admission in the US-VISIT context if you don't want to provide the biometrics) or may not exist. The specific opportunities to decline are described in the PIA or other relevant document published by the program through which the information is collected.

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

Whether an individual has a right to consent to a particular use of their data depends on the purpose of the collection which, if such a right exists, will be described in the PIA specific to the

program collecting the data. However, in most cases, because of the DHS national security, law enforcement, immigration, or DHS-mission related purposes for which the information is collected, no such right exists.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Notice with regard to the changes to IDENT necessitating this PIA are also discussed in a concurrently published IDENT SORN. The extent of notice and the opportunity to provide informed consent will vary based on the particular purpose associated with the collection of the information. In many law enforcement or national security contexts notice or the opportunity to consent would compromise the ability of the agencies to perform their mission. In these cases, notice and consent may not be available. However, many uses of IDENT data may require notice and consent. Each program will describe whether notice and consent are available, and if so how they are accomplished.

Section 7.0
Individual 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 which allow individuals to gain access to their own information?

Certain information may be exempt from individual access because access to 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 the 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. However, in other cases, individuals may request access to their data directly through the Redress process or other means as provided for in the PIA for each specific program collecting the data.

7.2 What are the procedures for correcting erroneous information?

Individuals may have an opportunity to correct their data when it is being collected; otherwise, they may submit a redress request as described by each program collecting the data or directly to the US-VISIT Privacy Officer who will refer the redress request to the appropriate program office.

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

Redress procedures are established and operated by the program through which the data was collected. In the case of redress requests for DHS organizations, if an individual is not satisfied with the response, an individual can appeal his or her case to the DHS Chief Privacy Officer, who will conduct a review and provide final adjudication on the matter.

7.4 If no redress is provided, are alternatives are available?

Redress procedures are established and operated by the program through which the data was collected. In the case of redress requests for DHS organizations, if an individual is not satisfied with the response, an individual can appeal his or her case to the DHS Chief Privacy Officer, who will conduct a review and provide final adjudication on the matter.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, what procedural rights are provided and, if access, correction and redress rights are not provided please explain why not.

The redress requests that might arise with respect to the various data collections stored in IDENT shall be addressed by the program through which the data was collected (e.g., DOS visa processing or US-VISIT).

Section 8.0
Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

DHS personnel and contractors will have access to the system. Personnel of other organizations will have access to their own information or to other information as described elsewhere in this or other PIAs. Specific user groups will be discussed in the PIAs published by each program collecting the data.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Some contractors will have access to the IDENT data. The extent of access will vary based on the need to fulfill the requirements of the contract under appropriate non-disclosure and use limitations. This will be defined in the associated PIA.

8.3 Does the system use "roles" to assign privileges to users of the system?

Access to IDENT is assigned based on the specific role of the users. Roles are created for each level of access required for individuals to perform their job functions. Examples of roles include basic user, system administrator, system auditor, and system manager.

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

DHS has documented standard operating procedures to determine which users may access IDENT. The minimum requirements for access to IDENT information are documented in security documentation, and include a DHS security clearance, security and privacy training, and need based on job responsibility.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The assignment of access roles varies based on the use or disclosure of IDENT data as described in the various PIAs. However, in most cases access roles are assigned by a supervisor and are reviewed regularly to ensure that users have the appropriate access. Individuals who no longer require access are removed from the access list. Access is audited and the audit logs are reviewed on a regular basis.

8.6 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 establishes 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.

Because IDENT contains data from a variety of sources, collected for a variety of uses, it is necessary to instantiate controls so that only those individuals making the appropriate use of the data are able to access that data. 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 in IDENT 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, a periodic assessment of physical, technical, and administrative controls is performed to enhance accountability and data integrity. External connections must be documented and approved with both parties signature in an ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

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

DHS requires that all users of IDENT data be trained on security and privacy issues. Some uses and sharing of IDENT data require system or program specific privacy training. Any specific privacy training would be defined in a specific system PIA or data sharing agreement.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The data is secured in accordance with DHS and national-level security requirements, including the FISMA requirements. IDENT was granted an authority to operate in May 2005, this authority to operate will expire in May of 2008 unless recreditation takes place beforehand.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

DHS has a robust security program that employs physical, technical and administrative controls. These controls are validated through a Certification and Accreditation process on a regular basis. Users have limited access that is established based on their role. Users are trained in the handling of personal information. The specific access controls for each use of information is described in the PIA relating to that use of information.

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 Was the system built from the ground up or purchased and installed?

IDENT was originally developed in 1994 as a biometrics collection and processing system for INS. It is comprised of standard commercial technology and customized hardware and software required to meet the needs of DHS.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

IDENT uses a privacy risk management process based on information life cycle analysis and fair information principles. Technical and programmatic design choices are informed by this approach, which analyzes proposed changes in terms of their life-cycle processes—collection, use and disclosure, processing, and retention and destruction—and the potential they may create for noncompliance with relevant statutes or regulations (the Privacy Act in particular) or for violations of fair information principles. When analysis determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed.

9.3 What design choices were made to enhance privacy?

IDENT was originally developed in 1994 as a biometrics collection and processing system for INS. Any changes that are made to IDENT are assessed using a privacy risk management process.

9.4 Privacy Impact Analysis: Given the above choices regarding technology, what privacy impacts were considered and how were they resolved?

The primary technical changes to IDENT have been the result of the maturation of the technical capability to match biometrics. As this capability matures it means that better matches can be made more quickly. Any new technology proposed for adoption by IDENT is assessed using a privacy risk management process. If any privacy risks are identified as part of this risk

management approach a determination is made whether an alternative technology or other appropriate technical, physical, or administrative control can be used to mitigate the risk.

Conclusion

While IDENT contains a significant amount of personal information, used for many purposes, applied in many environment, and used by a large number of users, nevertheless the privacy risks associated IDENT are minimal. DHS has created a rigorous security program employing physical, technical, and administrative controls to protect IDENT, in a way that would be difficult and excessively costly to implement if this data were contained in separate systems, in different locations, but that all must still link together to provide DHS' required functionality. DHS uses a privacy risk management process to ensure that all changes to IDENT do not significantly increase the risk to privacy.

Additional information on specific uses and disclosures will be found in PIAs for programs and systems that use IDENT data.

Responsible Officials

Steve Yonkers, US-VISIT Privacy Officer
Department of Homeland Security