Privacy Impact Assessment Update
for the

Enumeration Services of the

Automated Biometric Identification System (IDENT)

May 25, 2007

Contact Point
Claire Miller, Acting Privacy Officer
US-VISIT Program Office
(202) 298-5200

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

Abstract

The Automated Biometric Identification System (IDENT) is the primary repository of biometric information held by DHS in connection with its several and varied missions and functions, including but not limited to: the enforcement of civil and criminal laws (including immigration laws); investigations, inquiries, and proceedings in connection with those missions and functions; and national security and intelligence activities. IDENT is a centralized and dynamic DHS-wide biometric database. The Department of Homeland Security United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program is publishing this privacy impact assessment (PIA) update for the Automated Biometric Identification System (IDENT) to describe the changes to IDENT required to support enumeration services, a new service offering from IDENT. Enumeration services generates a unique personal identifier, known as an enumerator, for each individual for whom ten fingerprints and minimal biographic data has been collected in IDENT. Within IDENT the enumerator will be used to uniquely identify individuals and to link and retrieve immigration and border management records with a single identifier instead of multiple identifiers. This privacy impact assessment (PIA) has been conducted because the addition of enumerator services constitutes a significant change to IDENT.

Introduction

The Department of Homeland Security (DHS) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program is publishing this Privacy Impact Assessment (PIA) update for the Automated Biometric Identification System (IDENT) to provide information on how the new enumeration services feature of IDENT will impact privacy. IDENT is the primary DHS-wide system for the biometric identification and verification of individuals encountered in DHS mission-related processes. Because much of the DHS mission is associated with immigration and border management, most of the biometric and other personally identifiable information included in IDENT are of foreign nationals.

Enumeration services, a new service offering from IDENT, generates a unique personal identifier, known as an enumerator, for each individual for whom ten fingerprints and minimal biographic data has been collected. The enumerator is intended to uniquely identify an individual across the entire immigration and border management environment, but it is not intended to be used beyond that environment. The enumerator is a random number and has no inherent value; the digits (individually or in combination) of the enumerator are not "code" for any character, descriptor, or value. The enumerator is a raw and random number which only has meaning within IDENT or within the particular systems which may subscribe to enumerator services. IDENT will use the enumerator to uniquely identify an individual and ensure that all encounters included in IDENT are appropriately linked. The enumerator can then be used by IDENT user agencies for identification verification and linking of additional immigration and border

management documents. Enumeration services will enhance the reliability in establishing the unique identity of those persons encountered by the immigration and border management environment. This enhancement will provide a greater degree of confidence in the records retrieved and reduce the number of inadvertent misidentifications.

As the system owner of IDENT,[1] US-VISIT will be responsible for the operation and maintenance of the enumeration services, including serving as the owner of all generated enumerators. Enumeration services will be available to IDENT user agencies on individuals for whom ten fingerprints have been collected as part of a DHS immigration, law enforcement, or national security mission. That is to say, any agency that collects ten fingerprints from individuals, whether U.S. citizens, legal permanent residents, or foreign nationals, as part of its normal immigration, law enforcement, or national security mission, will be able to uniquely and efficiently identify individuals and their associated immigration and border management encounters in IDENT. All individuals with a set of ten fingerprints enrolled in IDENT will be enumerated. All user agencies may sign up for the enumerator service, but the enumerator and enumerator verification service will only be available to those user agencies that have entered into an agreement with US-VISIT.

The process is as follows: once ten fingerprints and limited biographic data are collected, a search of IDENT determines if an enumerated identity exists for the individual. If an enumerated record does not exist in IDENT, an enumerator will then be assigned to the individual. If an enumerated record does exist in IDENT, biometric and related biographic information are retrieved and provided to the appropriate decision maker for identity verification. The information retrieved is then linked to the individual's identity within IDENT. The enumerator represents a package of information held in IDENT. Upon subsequent encounters, the individual's identity may be verified using biometrics, along with other information previously collected and stored in IDENT.

The first client of enumeration services will be U.S. Citizenship and Immigration Services (USCIS), a DHS component. USCIS plans to use enumeration services as part of its Secure Information Management Service (SIMS) Pilot. SIMS is a case management service that will be used to enumerate individuals, including US citizens, to more accurately identify those within the USCIS inter-country adoption caseload.[2]

[1] 71 FR 42651, IDENT System of Records Notice, July 27, 2006.

[2] For further information on the privacy impact of USCIS SIMS pilot, refer to the *Privacy Impact Assessment for the USCIS Security Information Management Service (SIMS) Pilot* (DATE).

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?

Enumeration services does not collect new information for storage in IDENT. Enumeration services is an organizational tool for managing information that has already been collected and is contained in the IDENT system. It is also a tool for verifying identity.

An enumerator is a randomly generated alphanumeric unique identifier that is used to link disparate records associated with an individual. The enumerator is a new data element created within IDENT after an agency, through its normal business process, establishes an individual's identity through the collection of ten fingerprints and limited biographic information. An enumerator will neither contain embedded personally identifiable information, such as codes used to identify an individual, nor will the enumerator be derived from personally identifiable information. The enumerator will be a unique random number that will carry no information for anyone who does not have access to IDENT and enumeration services.

Enumeration services require the following previously collected data to create and assign an enumerator:

Biometric Data

- Ten fingerprints

Biographic Data

- First Name
- Middle Name, if applicable
- Last Name
- Date of birth
- Gender

The following data elements may be required where appropriate

- Document Type (including but not limited to a valid visa issued by a U.S. Consular Official, passport, personal identity card, drivers license and birth certificate)
- Document Number

- Document Issue Country
- Document Expiration Date

1.2 From whom is information collected?

No information is collected from individuals for enumeration services. Any individual who is enrolled in IDENT based on a collection of ten fingerprints and the biographic data described above will be enumerated. These are potentially any individuals who would be enrolled in IDENT as described in the previously published IDENT SORN and PIA.[3] From within DHS, data may have been collected from individuals by such agencies as Customs and Border Protection (CBP), United States Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE) 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) and other organizations that collaborate with DHS in pursuing national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

1.3 Why is the information being collected?

No information is collected for enumeration services. As an IDENT service offering, enumeration services helps to efficiently establish an individual's unique identity primarily during an immigration and border management encounter (e.g., border crossing, asylum application) or other encounter that supports a DHS mission, and then assigns an enumerator that links all IDENT records associated with that individual. This enhances officials' ability to quickly make informed decisions as to an individual's potential security risk and eligibility to receive a benefit, such as asylum, regardless of where, when, or with which agency the individual had been encountered. By enumerating only those individuals who submit ten fingerprints for storage in IDENT, DHS is able to enhance its ability to more accurately establish an individual's unique identity and thereby, with the use of an individual's enumerator, locate records on an individual with a greater degree of confidence and in a shorter period of time.

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. For example, see 69 Federal Register 2608-2615, United States Visitor and Immigrant Status Indicator Technology (US-VISIT) PIA, January 16, 2004.

[3] 71 FR 42651, IDENT System of Records Notice, July 27, 2006, IDENT Privacy Impact Assessment, July 31, 2006.

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.

Enumeration services do not involve the collection of new types of data and consequently no privacy concerns arise around new collection. However, even though new data is not collected, enumeration services produce new data in the form of an enumerator. The enumerator is designed to protect individual privacy and security. Specifically, the enumerator will be a randomly assigned alphanumeric identifier that neither contains embedded personally identifiable information, such as codes to identify an individual, nor will the enumerator be derived from personally identifiable information. The enumerator will be a unique random number that will carry no useful information for anyone who does not have access to IDENT and enumerator services.

DHS is moving toward collecting ten fingerprints rather than two fingerprints, as advocated by the National Institute of Standards and Technology (NIST), to improve accuracy in identification and verification of individuals. Although it is not anticipated that programs that currently collect two prints will switch to collecting ten fingerprints merely for the enumeration service, any privacy concerns associated with such a change would be covered by the PIA associated with that particular program.

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.

2.1 Describe all the uses of information.

Within IDENT, the enumeration service will be used to establish and verify the unique identity of an individual within the immigration and border management enterprise. Once a unique identity is established, then an enumerator will be assigned in order to link all encounters for that individual that have been included in IDENT. The enumerator can than be used by IDENT user agencies for identification verification and linking of additional immigration and border management documents. It is anticipated that the enumerator may be given to individuals to whom it applies. For example, an individual might present a document that contains that individual's assigned enumerator along with presenting biometrics in order to perform a one to

one match . This allows DHS to determine whether this is the same person DHS previously encountered with this identity.

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)?

US-VISIT uses analytic tools in its normal business process but it does not conduct data mining and the addition of enumeration services does not alter this. However, IDENT data may be used by others to support DHS national security, law enforcement, immigration, intelligence or other DHS mission-related functions. Any use of the data in this manner must be approved by the data owner, and it will be the responsibility of the data owner to describe such practices in the PIA and the SORN associated with the particular program.

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

Enumeration services does not collect additional information. The enumerator is a random number; it is not inherently accurate or inaccurate. Enumeration services uses data stored in IDENT. Because 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?), 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, the accuracy, completeness, and quality of data may vary considerably.

Enumeration services enhance the accuracy of the IDENT system because once an identity is established in IDENT, a randomly generated enumerator is assigned that will be used to link all records associated with this individual. This will significantly enhance the integrity of data, helping to ensure that the most accurate data will be tied to the correct person so that the appropriate decision is made or benefit is granted.

Enumeration services enhance the quality of the accuracy and data integrity checks already performed by IDENT (e.g., determining the quality of a fingerprint captured and its suitability for matching in the future). 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.

Enumeration services are distinct identification services that will use biometric and biographic data stored in IDENT to establish an identity and then assign a randomly generated enumerator. 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. It will be the responsibility of the data owner to document the proper use of, and controls on, the data by the user agencies.

One of the most significant concerns will be to prevent the misuse of the enumerator by unauthorized entities. Because the enumerator may be employed differently by each IDENT user, it will be necessary to ensure that each specific use of the enumerator will minimize the potential for misuse. Specifically, an individual's assigned enumerator may be made available to them on a document, for example, which may prove to be an attractive identifier by those entities unauthorized to use enumerators. Similarly there might be a concern that the enumerator would be used beyond the scope of its original purpose, for a national identification number for example. However, the enumerator is intended to uniquely identify an individual across the immigration and border management environment only; it is not intended to be used beyond the immigration and border management environment. Because the enumerator has no inherent value outside of IDENT, and the enumerator only represents information contained in IDENT, and most information in IDENT is not on US Citizens, the risk that the enumerator would become a national identifier is almost non-existent. It will be the responsibility of the data user to document this in the PIA or SORN associated with the particular IDENT use by an agency or program.

A concern inherent with assigning enumerators is that a potential border management environment-wide adoption of the service, including the distribution of these unique identifiers to individuals, will attract the attention of the private entities interested in using a ready-made individual identifier. Measures to prevent or mitigate any such misuse will be addressed in applicable agreements governing an agency's use of the information and described in the PIA for a particular program.

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. 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?

In accordance with the IDENT System of Records Notice (SORN) records associated with enumeration services will be retained until the statute of limitations has expired for all criminal violations or until they are older than 75 years.

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

The retention schedule for IDENT has been approved by NARA.

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

The retention period is 75 years (or until the end of the statute of limitations) 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 immigration. This is also tied to ENFORCE's retention period. IDENT hold the biometric information associated with the case management information in ENFORCE. Because ENFORCE needs to retain their data for 75 years to deal with potential immigration cases, IDENT needs to retain the supporting information for the same length of time.

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 with components throughout DHS. The enumerator may be shared with all DHS components that are using the enumeration service and that sign the enumeration services agreement with US-VISIT. Currently, it will only be shared with USCIS in a pilot project. USCIS will publish a PIA to detail their uses of the enumerator.

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

Enumerators will be shared with DHS components for use in identifying individuals and linking associated data. Data associated with an enumerator 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, 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?

When an enumerator is transmitted between IDENT and other systems on the DHS core network, it is done on an unclassified, secured wide area network. Other types of transmission or disclosure may be required in some circumstances in which case the mode of transmission or disclosure will be done in accordance with DHS policy, regulation and, if applicable, under the terms of an agreement executed between parties.

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 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. This includes controls that limit the use of the enumerator for uniquely identifying an individual within the immigration and border management environment only.

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?

Any agency using enumerators must be a subscriber to enumerator services. All such external sharing will be subject to applicable laws, regulation, memoranda of understanding, business rules and any other appropriate restraints on external data sharing. IDENT may share the enumerator with the same organizations that it shares any other type of IDENT data; i.e, Federal, state, local, tribal, foreign, or international government agencies engaged in national security, law enforcement, immigration, intelligence, and other mission-related functions, as determined by DHS.

5.2 What information is shared and for what purpose?

Those government entities that use the enumeration services will have access to individual enumerators in order to expediently link border management and immigration records stored in IDENT. The use of enumerators will be controlled by the underlying PIA for the entities' collection activity, as well as any executed Memoranda of Understanding (MOU) or other data sharing agreement between the parties. This includes controls that limit the use of the enumerator for uniquely identifying an individual within the immigration and border management environment only.

5.3 How is the information transmitted or disclosed?

Any agency using enumerators must be a subscriber to enumerator services. Enumerators will be 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 only data that is relevant and necessary to the other agencies mission may be transmitted directly between IDENT and those other systems; and
- Secure transfer, including encryption, on portable media when there is no direct connection between systems.

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

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 enters into MOUs or other agreements with all 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?

Enumeration services requires that external connections be secured and documented in an interconnection security agreement (ISA) that outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed. Organizations with which US-VISIT shares information must agree to maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information. Any federal agency with which US-VISIT shares information is required to handle the information in accordance with the Privacy Act and their applicable SORNs, and to the extent that the information is maintained electronically, consistent with Federal Information Security Management Act (FISMA). Furthermore, recipient organizations must notify US-VISIT after they become aware of any breach of security of interconnected systems, or potential or confirmed 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. This training may, in some cases, be provided by DHS. In other cases, it is the standard security and privacy training given by those organizations.

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. 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. This includes controls that limit the use of the enumerator for uniquely identifying an individual within the immigration and border management environment only.

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 creation of the enumerator does not impact collection of data. The extent of notice will vary depending on the particular collection. Any new collections of data associated with the enumerator will be covered in the collecting agency's PIA and may be covered in the Privacy Act statement if it is a voluntary 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. The IDENT SORN has also been updated to cover the storage and use of the enumerator.

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

The enumerator is not a collected data element, but rather a data element assigned *after* data is collected. The opportunity and/or right of individuals 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 or may not exist. The specific opportunities to decline are described in the PIA, SORN 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.

The data shared as part of enumeration services has been previously collected with the knowledge of the individual for the purposes of national security, law enforcement, immigration, intelligence, and other DHS-related missions. In most cases, individuals do not have any rights or opportunities to decline to share this data, or to consent to particular uses. US-VISIT, as the IDENT system owner, through its Privacy Officer, ensures that the privacy of all affected individuals is respected and responds to individual concerns raised about the collection of the required data.

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?

Enumeration services do not alter an individual's ability to access their information contained in IDENT as discussed in the IDENT PIA, July 27, 2006. IDENT 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, individuals may request access to their data directly through the Redress process as described below.

7.2 What are the procedures for correcting erroneous information?

Enumeration services do not result in any changes in the individual's IDENT redress process as discussed in IDENT PIA, July 27, 2006. 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 may 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 DHS through Traveler Redress Inquiry Program (DHS TRIP) which can be accessed at www.dhs.gov/trip.

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

Redress procedures are established and operated by the program through which the data are collected.

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.

Redress procedures are established and operated by DHS through Traveler Redress Inquiry Program (DHS TRIP) which can be accessed at www.dhs.gov/trip.

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 who have received the appropriate security and privacy training will have access to IDENT. The primary user groups include system managers, developers, and analysts. Access will be limited to the extent required for the particular user group to complete

their responsibilities. In instances where another Federal Agency uses IDENT pursuant to a MOU or some other agreement, those 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?

Contractors who have received the appropriate security and privacy training will have access to IDENT.

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

Access to IDENT is assigned based on the specific roles of the users. Roles are created for each level of access required for individuals to perform their official duties. 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 outlined in security documentation, and include a DHS security clearance, security and privacy training, and need to know based upon 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.

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 users, it is necessary to implement 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, 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 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 Federal security requirements, including the FISMA requirements. IDENT was granted an authority to operate in May 2007; this authority to operate will expire in May 2010

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

The development of the enumeration service has no affect on technical access and security issues relating to the IDENT system. DHS has a robust security program that employs physical, technical, and administrative controls. These controls are validated through a Certification and Accreditation (C&A) process on a regular basis. Users have limited access that is established based on their roles. 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 is comprised of standard commercial hardware and software which has been modified 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.

Policy, operational, and technical aspects were extensively analyzed to ensure that data integrity, privacy, and security protections were preserved in the deployment of enumeration services. 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?

The enumerator is designed to protect individual privacy and security. Specifically, the enumerator will be a randomly assigned alphanumeric identifier that neither contains embedded personally identifiable information, such as codes to identify an individual, nor will the enumerator be derived from personally identifiable information. The enumerator will be a meaningless identifier to those entities that do not have access to IDENT and enumerator services.

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

There are no significant technical changes to IDENT to support enumeration services. The enumerator itself is created in such a way that it contains no personal information, and no information can be derived from it. The enumerator must be entered into IDENT to derive any information.

Conclusion

This PIA has been prepared to explain the development of IDENT enumeration services. Enumeration services do not involve a change to the data collected or the populations covered in IDENT. Rather, enumeration services generate and verify a unique personal identifier, known as an enumerator. IDENT will use the enumerator to uniquely identify an individual and ensure that all encounters included in IDENT are appropriately linked. The enumerator can then be used by IDENT user agencies for identification verification and linking of additional immigration and border management documents related to that individual. The enumerator may be issued to individuals who have been enrolled in IDENT based on ten fingerprints and minimal biographic information. By enumerating only those individuals who are enrolled in IDENT based on ten fingerprints, which includes US citizens, legal permanent residents, and foreign nationals, DHS is able to enhance its ability to more accurately establish an individual's unique identity and thereby, with the use of an individual's enumerator, locate records on an individual with a greater degree of confidence and in a shorter period of time.

Because the enumerator is intended to uniquely identify all ten-fingerprinted individuals in IDENT there is the possibility that if the enumerator is available to the unauthorized individuals, perhaps on documents, the enumerator could be attractive for use by unauthorized entities in identifying individuals. This risk will be mitigated by the IDENT user agencies as documented in agreements between the user agencies and IDENT; it is the responsibility of the user agency to document these agreements in the PIA.

In the event changes are made to enumeration services that require a modification to this PIA, a revised PIA will be published. Additional information on specific uses and disclosures will be found in PIAs for programs and systems that use IDENT data.

Responsible Officials

Claire Miller, US-VISIT Acting Privacy Officer
Department of Homeland Security

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security