Privacy Impact Assessment
for the

Interim Data Sharing Model (iDSM)
for the Automated Biometric Identification System (IDENT)/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability Project

September 1, 2006

Contact Point
Steve Yonkers, Privacy Officer
US-VISIT Program Office, Department of Homeland Security
(202) 298-5200

Reviewing Official
Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The Automated Biometric Identification System (IDENT) Privacy Impact Assessment (PIA), published on July 26, 2006, describes IDENT as 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. The IDENT PIA provides the baseline for how IDENT data is appropriately controlled and safeguarded. Furthermore, the IDENT PIA describes how IDENT shares data with Federal, state, local, tribal, foreign, or international government agencies charged with DHS mission-related functions.

As anticipated under the External Data Sharing section of the IDENT PIA, this document discusses the sharing of data between IDENT and the Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Criminal Justice Information Service (CJIS) Division's Integrated Automated Fingerprint Identification System (IAFIS). FBI/CJIS provides criminal history information to Federal, state, and local law enforcement agencies. The FBI completed its own PIA on the data it shares with IDENT. Therefore, this PIA discusses only the DHS sharing of IDENT data with the FBI/CJIS.

Introduction

Consistent with guidance issued by the Office of Management and Budget (OMB) and policy guidance issued by the DHS Privacy Office, this PIA is being prepared by the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program as the system owner of IDENT to address a sharing of data with the DOJ's FBI/CJIS Division's IAFIS. While US-VISIT is the system owner of IDENT, the actual data in IDENT is owned and controlled by the organization that collected it. Consistent with the IDENT PIA, DHS may share IDENT data with the consent of the data owner for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions, as determined by DHS.

DHS and DOJ are jointly developing the IDENT/IAFIS Interoperability Project (Interoperability). The requirement for interoperability between these systems comes from various legislative and administrative mandates including the conference report for DHS's Appropriation Bill for FY 2004, the conference report for the DOJ's Consolidated Appropriations Act for FY 2005, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, the Homeland Security Act of 2002, the Enhanced Border Security and Visa Reform Act (Border Security Act) of 2002, and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. The interim Data Sharing Model (iDSM), which is the first of three phases of Interoperability, establishes the platform and processes necessary to support limited data sharing and will act as the first step toward more extensive sharing. In this phase the data to be shared is limited to two data sets: data on immigration

violators provided by Immigration and Customs Enforcement (ICE) and data on certain critical visa refusals provided by the Department of State (DOS). The ICE data is currently shared with law enforcement agencies using a manual exchange method that is less secure than iDSM. The provision of DOS data to FBI/CJIS constitutes a new data sharing activity. Once fully deployed, Interoperability is intended to provide seamless bi-directional sharing of data between IDENT and IAFIS to support the law enforcement, national security, and immigration control missions of both DOJ and DHS. This PIA will be updated to address the sharing of additional IDENT data sets and/or the implementation of future Interoperability phases.

The iDSM will support the sharing of a specific limited set of IDENT data for FBI/CJIS's use and the sharing of IAFIS data for DHS's use for the purpose of biometric matching. This will be accomplished by creating the technical and procedural infrastructure so DHS and FBI can provide each other access to a defined set of biometric and biographic data. Each party may then biometrically search against the shared data and, if a match is found, request additional information.

The iDSM provides DHS access to IAFIS data through a FBI/CJIS-provided subset of IAFIS. The FBI/CJIS is provided access to the IDENT data through a subset of IDENT data stored by FBI/CJIS. The data sharing approach selected for iDSM was implemented in response to the Congressionally-mandated timeline for Interoperability implementation and technical feasibility. As iDSM is implemented in phases, DHS and DOJ will review this implementation. The IDENT data stored by FBI/CJIS will consist of two data sets: data on immigration violators provided by ICE and data on certain critical visa refusals provided by DOS. As anticipated by the IDENT PIA, this iDSM phase of Interoperability is being documented to address the sharing of these specific IDENT subsets with FBI/CJIS. The data shared by IAFIS with DHS comprises certain individuals in the Subject Criminal Master File.

In order to biometrically identify individuals using IDENT data, FBI/CJIS will run a query using its fingerprint and biographic data against the IDENT data stored by FBI/CJIS. The query result will be returned to FBI/CJIS. Any positive match responses are then forwarded to the ICE Law Enforcement Support Center (LESC) for data verification and interpretation.

For the purposes of the iDSM phase, the FBI/CJIS users of the biometric identification service will also include the Boston Police Department and the Texas Department of Public Safety for law enforcement purposes, and the U.S. Office of Personnel Management (OPM) for background security investigations for individuals seeking Federal employment.

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?

The subset of IDENT data stored by FBI/CJIS will provide IAFIS users access to data collected by ICE on immigration violators and data provided by DOS on certain critical visa refusals. The data to be shared is limited to:

- DHS Unique Identification Number,
- FBI Fingerprint Number (FNU), if available,
- Fingerprint image,
- Date of birth,
- Place of birth,
- Gender; and
- Subject name.

1.2 From whom is information collected?

The provision of IDENT data to IAFIS users through the iDSM does not involve any changes in the information currently stored in IDENT. ICE data included in the IDENT data stored by FBI/CJIS comes from information collected from immigration violators. DOS data included in the IDENT data stored by FBI/CJIS comes from individuals who have been denied certain visas.

1.3 Why is the information being collected?

Data collection is not an activity of the iDSM phase of Interoperability. The iDSM phase of Interoperability facilitates the sharing of previously collected data stored in IDENT with FBI/CJIS users. The purposes for which data was collected are discussed in the IDENT PIA in support of DHS carrying out its national security, law enforcement, immigration, intelligence, and other DHS-related missions.

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]

The requirement for interoperability between these systems comes from various legislative and administrative mandates, including the conference report for DHS's Appropriation Bill for FY 2004, the conference report for the DOJ's Consolidated Appropriations Act for FY 2005, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, the Homeland Security Act of 2002, the Enhanced Border Security and Visa Reform Act (Border Security Act) of 2002, and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004.

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.

The sharing of IDENT data with FBI/CJIS users does not involve a change to the type of data collected, the individuals from whom it is collected, the purpose for which data is collected, or the authority to collect data as discussed in the IDENT PIA. Consequently, no new privacy risks have been identified with regard to data collection.

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.

Through the iDSM phase of Interoperability, FBI/CJIS users will have access to the specified IDENT data sets only in support of DHS-related missions. The Boston Police Department and the Texas Department of Public Safety for law enforcement purposes, and OPM for background security investigations for individuals seeking Federal employment, will use the IDENT data in CJIS to

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

biometrically identify immigration violators as determined by ICE and certain individuals denied visas by DOS.

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)?

No data mining is conducted.

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

As discussed in the IDENT PIA, IDENT performs certain data quality checks and seeks to ensure that the data stored in IDENT meets a minimum level of quality and completeness. All data owners are responsible for ensuring the accuracy, completeness, and quality of their data.

CJIS users of the IDENT data stored by FBI/CJIS must receive data verification and interpretation of IDENT data from the ICE LESC prior to taking any action based on that 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.

In order to assure that IDENT data stored by FBI/CJIS is used appropriately, FBI/CJIS users must receive data verification and interpretation of IDENT data from the ICE LESC prior to taking any action based on that data.

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?

The retention period for IDENT data has not been changed. The provision of IDENT data for storage by the FBI/CJIS is contingent upon that data continuing to be held in IDENT. Therefore, the retention period for the IDENT data stored by FBI/CJIS will comply with the IDENT System of Record Notice (SORN), which specifies that data for which the statute of limitations has expired for all criminal violations or that are older than 75 years will be purged.

IDENT data that is shared with FBI/CJIS users will be maintained in accordance with the FBI/CJIS users' retention schedules.

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 the National Archives and Records Administration (NARA).

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

The IDENT data stored by FBI/CJIS is controlled by DHS. When IDENT records reach their 75 year retention limit, they will be automatically deleted from the FBI/CJIS system. The FBI/CJIS users will incorporate the IDENT data into their case files. These case files are retained according to each user's specific record retention schedule. The IDENT data maintained in the case files is under the control of the specific FBI/CJIS users and is maintained in accordance with their records management programs. This creates a low risk that the data may not be updated in a timely manner for processing new encounters with an individual. Because each new encounter results in a new query against IDENT, the risk of new decisions being made on outdated data is low. Also, all case files are classified as law enforcement sensitive and are protected by appropriate physical, administrative, and technical controls.

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?

DHS components do not use iDSM. DHS components are required to access IDENT data through the standard IDENT process as discussed in the IDENT PIA.

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

DHS components do not use iDSM. DHS components are required to access IDENT data through the standard IDENT process as discussed in the IDENT PIA.

4.3 How is the information transmitted or disclosed?

DHS components do not use iDSM. DHS components are required to access IDENT data through the standard IDENT process as discussed in the IDENT PIA.

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

DHS components do not use iDSM. DHS components are required to access IDENT data through the standard IDENT process as discussed in the IDENT PIA. Therefore, there are no additional risks associated with internal sharing of IDENT data.

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 governments, and the private sector.

5.1 With which external organizations is the information shared?

The IDENT data stored by FBI/CJIS will consist of two data sets: data on immigration violators provided by ICE and certain critical visa refusals provided by DOS. FBI/CJIS users of this IDENT subset is limited to the Boston Police Department and the Texas Department of Public Safety for law enforcement purposes, and OPM for background security investigations for individuals seeking Federal employment.

5.2 What information is shared and for what purpose?

The IDENT data stored by FBI/CJIS will provide FBI/CJIS users access to data provided by ICE on immigration violators and data provided by DOS on certain critical visa refusals. The data to be shared is limited to:

- DHS Unique Identification Number,
- FBI Fingerprint Number (FNU), if available,
- Fingerprint image;
- Date of birth;
- Place of birth;
- Gender; and
- Subject name.

5.3 How is the information transmitted or disclosed?

In order to biometrically identify individuals using IDENT data, FBI/CJIS will run a query using its fingerprint and biographic data against the IDENT data stored by FBI/CJIS. The query result will be returned to FBI/CJIS. Any positive match responses will then be forwarded to the ICE LESC for data verification and interpretation.

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?

Letters of Concurrence (LOCs) between DHS and DOJ , as well as a number of jointly developed system documents, reflect the scope and specific controls on Interoperability data sharing, including governing the protection and use of the data for the iDSM phase. In turn, FBI/CJIS has data sharing agreements with users having access to IDENT data through the IDENT data stored by FBI/CJIS to ensure that data is accessed and used appropriately. DHS has determined that these agreements support the limitations established for the use of IDENT data.

5.5 How is the shared information secured by the recipient?

IDENT data stored by FBI/CJIS is secured in accordance with the DOJ Certification and Accreditation (C&A) processes. IDENT data shared with FBI/CJIS users is secured according to the protection regimen established by each user.

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

FBI/CJIS provides privacy and security training to its users accessing IDENT data stored by FBI/CJIS. In addition, FBI/CJIS users have experience in handling similar types of data to which they currently have access, and any potential match will be followed up using established procedures for engaging the ICE LESC to verify and interpret the match.

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

LOCs between DHS and DOJ, as well as a number of jointly developed system documents, reflect the scope and specific controls on Interoperability data sharing, including governing the protection and use of the data for the iDSM phase. In turn, FBI/CJIS has data sharing agreements with users having access to IDENT data stored by FBI/CJIS. In addition, to ensure IDENT data is

used appropriately, FBI/CJIS users of the IDENT data stored by FBI/CJIS must receive data verification and interpretation of IDENT data from the LESC prior to taking any action based on that data.

Section 6.0
Notice

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

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?

Notice is provided by means of the publication of the IDENT PIA, the IDENT SORN, and this iDSM PIA on the DHS website and in the Federal Register.

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

The IDENT data shared with FBI/CJIS users has previously been collected from immigration violators provided by ICE and data on certain critical visa refusals provided by DOS. Individuals do not have the opportunity or right to decline to provide the data processed and shared for the iDSM based on the collection purposes of DHS national security, law enforcement, immigration, intelligence, or other DHS-related purposes.

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?

The collected data is used only for the purposes of national security, law enforcement, immigration, intelligence, and other DHS-related mission purposes, as defined by DHS. Individuals have no opportunity to consent to or refuse the use of this data for any of these purposes. Individuals seeking Federal employment requiring a background security investigation by OPM provide specific consent for the search of all DHS records.

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 using the iDSM 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. The iDSM shares data for these same purposes. 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?

The iDSM does not result in any changes in the individual's ability to access their information contained in IDENT as discussed in the IDENT PIA.

7.2 What are the procedures for correcting erroneous information?

The iDSM does not result in any changes in the individual's IDENT redress process as discussed in the IDENT PIA.

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

The iDSM does not result in any changes in the process for notifying individuals of the procedures for correcting information contained in IDENT as discussed in the IDENT PIA.

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

Redress opportunities are provided.

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.

Because the data stored in IDENT and shared with FBI/CJIS users is largely for law enforcement purposes, there are significant limits on the rights of individuals to access the data. As discussed in the IDENT PIA, IDENT has an existing redress process to correct erroneous data stored in its system. However, in most cases the data owner would be required to correct the data. ICE is the owner of immigration violator data and DOS is the owner of critical visa refusal data. DHS will collect these requests and forward them to the appropriate organization, or the requester will be notified of the appropriate processing agency for the request.

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?

FBI/CJIS users are provided access to IDENT data through a subset of IDENT data stored by FBI/CJIS. As discussed in the IDENT PIA, select DHS personnel and contractors will have access to the system, as required. Data owners may provide their personnel and contractors access to data in IDENT as allowed by the IDENT PIA and the PIA of the original data source.

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 may 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 nondisclosure and use limitations.

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

IDENT assigns access privileges 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.

FBI/CJIS users of the IDENT iDSM are not provided direct access to the IDENT data.

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 the IDENT system. The minimum requirements for access to IDENT system 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?

The iDSM will secure 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 that are applied to component systems, communications between component systems, and all interfaces between component systems and external systems. The security policy also requires that all users be adequately trained regarding the security of their systems, and a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity. All system users must complete security training. External connections must be documented and approved with both parties' signatures in an interagency security agreement (ISA) outlining 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?

FBI/CJIS provides limited privacy and security training to the users of IDENT data. In addition, FBI/CJIS users have experience in handling similar types of data to which they currently have

access to, and any potential match will be followed up using established procedures to verify and interpret the match.

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

The IDENT data stored by FBI/CJIS will be secured in accordance with DHS and Federal security requirements, including the FISMA requirements. The IDENT C&A documentation will be updated to include the iDSM, including a full security risk assessment. IDENT is operating under an authority to operate which expires in May 2008. The data stored by FBI/CJIS will be secured in accordance with DOJ and Federal security requirements, including the FISMA requirements.

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

The iDSM will maintain an appropriate level of security in accordance with the sensitivity of the data and the requirements of the data owners. A complete security risk assessment will be conducted and a determination will be made whether security risks have been properly mitigated.

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?

The iDSM is an extension to existing systems, IDENT and IAFIS, and is based on commercial-off-the-shelf hardware and software that has been modified to meet the needs of this particular implementation.

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

Extensive policy, operational, and technical discussions were held to ensure that data integrity, privacy, and security were analyzed in the development of the iDSM. As this is the first phase of Interoperability, ongoing testing and validation of assumptions will allow for additional privacy enhancements to be made.

9.3 What design choices were made to enhance privacy?

The iDSM provides for only a limited sharing of appropriate data. In addition, rather than directly sharing all data, the iDSM relies on limited sharing of data, plus additional validation beyond the sharing to ensure that the data is correctly interpreted and used.

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

The risks of sharing IDENT data with FBI/CJIS are significantly mitigated through limitation of the data being shared, minimizing data access, implementing data verification processes, and having the ability to automatically update data IDENT data stored by FBI/CJIS.

Conclusion

The iDSM does not involve a change to the data collected or the populations covered in IDENT. It is a new method for sharing existing data between IDENT and IAFIS for DHS law enforcement and national security purposes. This sharing is mandated by law and conforms to appropriate uses as indicated at the collection of the data and documented in the IDENT SORN. Before any of the data shared in the iDSM is used, it will be separately validated to ensure its accuracy and currency. Any security risks identified during implementation will be appropriately mitigated to help ensure privacy. As additional phases of Interoperability are implemented, this PIA will be updated as necessary.

Responsible Officials

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