



**Privacy Impact Assessment Update
for the**

**Biometric Interoperability Between the
U.S. Department of Homeland Security
and the U.S. Department of Justice**

DHS/NPPD/USVISIT/PIA-007(b)

October 13, 2011

Contact Point

Paul Hasson

Privacy Officer

US-VISIT Program

National Protection and Programs Directorate

202-298-5200

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

In 2006, the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program of the Department of Homeland Security (DHS) and the Criminal Justice Information Services (CJIS) Division of the Federal Bureau of Investigation (FBI), Department of Justice (DOJ), developed an interoperability project to support the sharing of information among DHS, DOJ, and their respective stakeholders. This Privacy Impact Assessment (PIA) update is being conducted to reflect the expansion of DHS–DOJ interoperability to include users and uses not previously covered under the *interim Data Sharing Model (iDSM) for the IDENT/IAFIS Interoperability Project (iDSM)* and *First Phase of the Initial Operating Capability (IOC) of Interoperability between the DHS and the DOJ PIA (IOC)* PIAs. In addition, DHS-DOJ Interoperability is expanding to allow approved users access to a more comprehensive IDENT response, containing up to all data fields captured in IDENT.

Introduction

Developed in 2006, DHS-DOJ Interoperability allows an approved user to submit a single query and receive results from the US-VISIT Automated Biometric Identification System (IDENT) and the DOJ Integrated Automated Fingerprint Identification System (IAFIS) rather than submitting two separate queries. Through this “Shared Services” model, a user submits a query to CJIS who sends the query to IDENT. If the user requests a “search only” response, no data is retained in IDENT and IDENT returns the “match” or “no match” response along with the authorized data elements. If the user requests “search and enroll,” IDENT stores the query, sends back the match or no match response, and when new encounters occur, provides wrap-back notifications.¹

On September 1, 2006, US-VISIT published the iDSM PIA which initiated groundwork for the project. On October 23, 2008, US-VISIT published the IOC PIA.² The IOC PIA outlined the implementation of the first phase of the IOC. Since then the capability has expanded to cover additional stakeholders, data sharing, and services. DHS–DOJ interoperability has moved beyond the first phase of IOC and continues to expand its potential base of users and to improve processes and functionality in support of the anticipated full interoperability capabilities outlined in the IOC PIA. It is expected that additional agencies will be granted access to IDENT and IAFIS/Next Generation Identification (NGI), although that access will occur incrementally, as resources permit.

¹ Wrap-back functionality allows customers to specify events or a condition for automatic notification when a subject meets a pre-established system parameter, such as if a subject reaches a particular watch list level. The customer must enroll their data as “search and enroll” to receive wrap-back. Once CJIS receives the IDENT response, CJIS packages the IDENT and IAFIS response and returns the entire response to the user.

² See *interim Data Sharing Model (iDSM) for the Automated Biometric Identification System (IDENT)/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability Project Privacy Impact Assessment (PIA)* and the *First Phase of the Initial Operating Capability (IOC) of Interoperability Between the DHS and the DOJ PIA* at www.dhs.gov/privacy.



Initially, the deployment of DHS–DOJ interoperability to new users was focused on law enforcement agencies, particularly those at the state and local levels. However, because of specified new-user qualification standards, other criminal justice, non-criminal justice, and Intelligence Community users are being added, when possible. Along with these new-user qualification standards, DHS and DOJ have instituted an integrated project team (IPT) and a strategic policy team (SPT) to establish a strict application process such that DHS and DOJ may identify all potential new users and establish their authority to receive data based on their mission needs and routine uses.

Through a thorough review process discussed in the *External Sharing* section of this PIA Update, the IPT and the SPT review the information in the application and determine whether the new user will be approved and what information the user may receive in a response. In some instances, a new user may be better suited for direct connectivity to the two systems rather than a DHS-DOJ Interoperability connection, and in that case the user will be denied access through Interoperability. In other instances, the user may not have the inherent authority to receive the information in the systems and therefore will be denied.

In addition to the inclusion of new users, based on user needs and authorization to receive specified data fields, DHS–DOJ interoperability has expanded to allow approved users access to a more comprehensive IDENT response containing up to all data fields captured in IDENT, as discussed in *The System and the Information Collected and Stored in the System* below.

Reason for the PIA Update

This update covers the expanded sharing with the Department of Justice (DOJ), Federal Bureau of Investigation (FBI) special agents using the Quick Capture Platform (FBI Mobile), DOJ FBI Bioterrorism Risk Assessment Group (FBI/BRAG), DOJ FBI Special Identities Unit (SIU), and the Office of Personnel Security and Suitability, Diplomatic Security, U.S. Department of State (DOS/SI/OPSS).

In addition, DHS-DOJ Interoperability is expanding to allow approved users access to a more comprehensive IDENT response, containing up to all data fields captured in IDENT as described below in the *System and the Information Collected and Stored in the System* section. Under the iDSM and IOC PIAs, users were only able to receive basic biographic data elements.

Unless otherwise noted, the information provided in the September 1, 2006 iDSM PIA and the October 23, 2008 IOC PIA remain in effect. Individuals are encouraged to read the iDSM PIA, IOC PIA, and this PIA update to have a complete understanding of US-VISIT's privacy analysis of DHS–DOJ interoperability activities.



Privacy Impact Analysis

The System and the Information Collected and Stored in the System

IDENT receives biometric and associated biographic data from DHS and external stakeholders to conduct biometric searches against IDENT. At the request of a stakeholder, IDENT also may store biometric and associated biographic data that varies for each stakeholder, but which in general may consist of:

(a) Biometric Data:

- photographs;
- fingerprints (including DHS and other agency fingerprint record locator information); and
- other biometric modalities to be added in the future (e.g., iris and facial images).

(b) Biographic Data:

- name;
- date of birth;
- gender;

(c) Personal identifiers, including but not limited to:

- alien number (A-number);
- Social Security number (if available);
- state identification number (SID);

(d) Personal physical details, such as height, weight, eye color, and hair color;

(e) Fingerprint identification number (FIN);

(f) FBI record identifier;

(g) Details for citizenship and nationality, including person-centric details that may be biographic and biometric;

(h) Derogatory information, if applicable, including:

- wants and warrants;
- known or suspected terrorists (KSTs);
- sexual offender registration;



- immigration violations; and
 - identity watchlist status information.
- (i) Miscellaneous comment information;
- (j) Document information, including passport and visa data;
- (k) Encounter Data:

Transaction-identifier data includes:

- the sending organization;
- timestamp;
- reason sent, such as entry, visa application, credentialing application, or apprehension;
- and any available encounter information, including encounter identification number(s) when applicable.

The expansion of DHS–DOJ interoperability now allows authorized users who have an approved need to know for a specific authorized use to receive up to a full IDENT response. The response will include data fields that the user requests which they are also authorized to have.

In contrast, the initial deployment of DHS–DOJ interoperability provided a limited response. The data elements in that response included full name, date of birth, place of birth, gender, photograph, and DHS system record locator.

Uses of the System and the Information

Uses of the system and information have not changed.

Retention

The retention schedules have not changed.

Internal Sharing and Disclosure

As discussed in the October 23, 2008 IOC PIA, because IDENT is the primary DHS-wide repository for biometrics, data maintained in IDENT may be shared throughout DHS for mission-related purposes.

Through interoperability, IDENT data is currently shared with authorized users for the following purposes: national security, law enforcement, immigration and border management, and intelligence, and to conduct background investigations for national security positions and certain positions of public trust.



This update covers the expanded sharing with the DOJ, FBI special agents using FBI Mobile, FBI/BRAG, FBI SIU, and DOS/SI/OPSS.

FBI Mobile Interoperability Initiative

The FBI Mobile Interoperability Initiative allows FBI personnel to capture biometric samples in field settings for submissions to IAFIS and IDENT through the FBI's Quick Capture Platform (QCP) device. FBI Mobile submits data as search-only, so the data is not stored in IDENT and FBI Mobile users do not receive wrap-back notifications.

FBI Mobile receives all of the above listed data elements in IDENT except:

- fingerprints;
- other biometric modalities;
- FIN; and
- FBI Record Identifier.

This sharing of personally identifiable information (PII) outside of DHS is compatible with the original collection of that information and is covered by the IDENT SORN, 72 FR 31080 (June 5, 2007).

All or a portion of the data contained in IDENT records may be disclosed as a routine use under 5 U.S.C. § 552a(b)(3) to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions as determined by DHS (Routine Use A).

FBI Bioterrorism Risk Assessment Group

FBI BRAG's role is to enhance national security and public safety by providing the timely and accurate determination of an individual's eligibility to use, possess, or transfer select biological agents and toxins. Candidates are evaluated for access to select agents and toxins against criteria delineated in the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, and against prohibitive categories defining a restricted person in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). BRAG submits data as search-only, so the data is not stored in IDENT and FBI BRAG users do not receive wrap-back notifications.

FBI BRAG receives all data elements listed above with the exception of:

- fingerprints;
- other biometric modalities;



- FIN; and
- FBI Record Identifier.

The sharing of PII outside of DHS is compatible with the original collection of that information and is covered by the IDENT SORN, 72 FR 31080 (June 5, 2007).

All or a portion of the data contained in IDENT records may be disclosed outside DHS as a routine use under 5 U.S.C. § 552a(b)(3) as part of a background check or security screening in connection with hiring, retention, performance of a job function, or issuance of a license or credential (Routine Use B).

FBI Special Identities Unit

The mission of the SIU is to enhance national security by identifying and locating threats to the United States through subject-of-interest queries. SIU submits data as search-only, and therefore the data sent is not stored in IDENT and SIU does not receive wrap-back notifications.

SIU receives all data elements listed above with the exception of:

- fingerprints;
- other biometric modalities;
- FIN; and
- FBI Record Identifier.

The sharing of PII outside of DHS is compatible with the original collection of that information and is covered by the IDENT SORN, 72 FR 31080 (June 5, 2007).

All or a part of the data contained in IDENT records may be disclosed as a routine use under 5 U.S.C. 552a(b)(3) to appropriate federal, state, local, tribal, foreign, or international agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions as determined by DHS (Routine Use A).

Office of Personnel Security and Suitability

OPSS is the Office of Personnel Security and Suitability, Diplomatic Security, U.S. Department of State (DOS/SI/OPSS). The mission of the DOS personnel security program is to assure that granting an individual access to classified information is clearly consistent with the interests of national security. To fulfill its mission, the OPSS conducts for both applicants and incumbents for the Foreign Service, Civil Service and a variety of type of contractor hires, which include foreign nationals and dual citizens. OPSS also provides support to those non-criminal investigations conducted to support locally employed staff positions, which are managed by



Regional Security Officers within the Bureau of Diplomatic Security and located at Embassies and Consulates around the world.

OPSS plays an important role in the hiring process by providing investigations to assist in determining an applicant's initial, or an incumbent's continued, suitability for employment and ability to hold access to information. The office conducts over 35,000 personnel security investigations each year. OPSS submits data as search and enroll and therefore the data is stored in IDENT and OPSS receives wrap-back notifications.

OPSS receives all data elements listed above.

The sharing of PII outside of DHS is compatible with the original collection of that information and is covered by the IDENT SORN, 72 FR 31080 (June 5, 2007).

All or a portion of the data contained in IDENT records may be disclosed outside DHS as a routine use under 5 U.S.C. § 552a(b)(3) as part of a background check or security screening in connection with hiring, retention, performance of a job function, or issuance of a license or credential (Routine Use B).

Privacy Risks and Mitigation

Because of the expansion of data available in an IDENT response, there is a risk that more data fields than needed will be shared with an authorized user. To mitigate this risk, DHS and DOJ have instituted the IPT and SPT to establish a strict application process so that DHS and DOJ may identify all potential new users and establish their authority to receive data based on their mission needs and routine uses. As defined in the *Improved Information Sharing Services Memorandum of Understanding* (Interoperability MOU) dated July 1, 2008, all new users must qualify as "authorized users" and justify their "need to know" the information for an "authorized use." This includes determining the appropriateness of the information shared. For example, some users may only need a limited subset of the information in IDENT while others may require the full IDENT response. A new user must be reviewed and approved by DHS on a case-by-case basis to determine whether an appropriate use, in accordance with the DHS mission, exists before allowing a query of, and an appropriate response from, IDENT for the new user.

As part of the IPT, all new user applications go through the User Evaluation and Deployment Process to identify and define new users, potential new uses, and requested responses. The application process begins with the potential new user presenting an initial request for services to CJIS who presents the application to the IPT. The application includes sections, for example, that require a statement of the proposed use and benefits of sharing IDENT and IAFIS/NGI data, the reason a user may need to receive a specific data element, and the executive order, statute, or regulation that grants the authority to receive IDENT data. Questions are formulated by US-VISIT, CJIS, DHS, and the DOS. The potential user and/or



sponsoring party provide responses. At the SPT, analysis is done by US-VISIT, DHS, DHS Screening and Coordination Office (SCO), and DOS to determine if the new user is authorized. A recommendation is made and discussed at the next IPT. At the IPT, analysis is done by all interested parties including CJIS to determine if the new user is authorized and a recommendation is made. The recommendation is then sent to senior US-VISIT leadership who will determine the accuracy of the proposed recommendation. This recommendation will then be routed through the US-VISIT internal Executive Secretary review process for awareness and concurrence. The Executive Board (EB), a panel made up of senior DHS, DOJ, and DOS officials, reviews the recommendation. If the request needs department level review it will be sent to NPPD Information Sharing Governance Board (ISGB). If further approval is needed the request is forwarded to the DHS Executive Stakeholders Board (ESB). The IPT is notified of the decision. The request is vetted through the DHS ISGB stakeholders (DHS Privacy, CRCL, OGC). The EB or the ESB will relay their decision to the potential new user through the IPT.

As DHS-DOJ interoperability continues to expand, there is also a risk that a user authorized to request/obtain information for a specified use will use the access for inappropriate purposes. US-VISIT mitigates this risk by implementing access controls to ensure that only authorized users can access the data and that this access is in line with authorized uses. The applicable data-sharing agreements require the proper authorization of new users and uses. All approved users must ensure that appropriate authorization exists before the use of DHS-DOJ interoperability is initiated. It is the responsibility of all parties to the data-sharing agreements to require proper authorization for all users, to ensure that uses are applicable in terms of their authorized access, and to verify that such authorizations exist before a search request is entered into the other party's system.

Additionally, to inform new users of compliance requirements, US-VISIT is currently developing an *On-Boarding Package* to be distributed to all new users that covers privacy compliance requirements as well as the relevant terms of the Interoperability MOU. CJIS also provides limited privacy and security training to its authorized users of IDENT data.

The risk is also mitigated by the US-VISIT Program Assessment Compliance and Evaluation Team conducting compliance reviews (internal compliance auditing), as appropriate, on the use of the data with authorized users. The Interoperability MOU dictates an additional layer of review that, in addition to regular audit schedules, any party may make a request for a copy of the audit log of another party to ensure compliance.

There is a risk that the user will inappropriately share data received through DHS-DOJ Interoperability. As DHS-DOJ Interoperability users, SIU, FBI Mobile, BRAG, and OPSS must all comply with third-party disclosure rules. Before any information originating from IDENT may be disclosed to a third party, US-VISIT must be contacted to determine the appropriate



action or response, unless such third-party sharing occurs with other U.S. law enforcement agencies as part of the routine course of an active law enforcement investigation.

In addition, the US-VISIT Program Assessment Compliance and Evaluation Team will conduct periodic auditing for compliance within the program and externally with CJIS to ensure that the information is used in accordance with stated acceptable uses documented in the Interoperability MOU and Privacy Compliance documentation.

Notice

General notice is provided through this PIA update.

Individual Access, Redress, and Correction

Access, redress, and correction have not changed with this update.

Technical Access and Security

IDENT received a 3-year authority to operate on May 4, 2010.



Technology

IDENT functionality is managed through detailed IDENT Exchange Messaging (IXM) services, which are configurable based on the user, user needs, and user permissions. IXM employs applicable filters that have been installed in IDENT to allow for the suppression of encounter-specific and data element-specific information in IDENT responses, based on the requesting entity and the encounter owner's business rules for data sharing.

Responsible Official

Paul Hasson, US-VISIT Privacy Officer

NPPD/US-VISIT

Department of Homeland Security

Approval Signature

[Original signed copy on file with the DHS Privacy Office]

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security