



Privacy Impact Assessment  
for the

**Identity Intelligence Biometrics (I2B) Pilot**

**DHS/ALL/PIA-054**

**October 13, 2015**

**Contact Point**

**Benjamin Stefano**

**Senior Advisor, Office of Intelligence and Analysis**

**Department of Homeland Security**

**(202) 282-8646**

**Reviewing Official**

**Karen L. Neuman**

**Chief Privacy Officer**

**Department of Homeland Security**

**(202) 343-1717**



## Abstract

The Identity Intelligence Biometrics (I2B) pilot is intended to develop a cloud-based multi-modal (face and fingerprint) automated biometric identification system using non-U.S. person biometric records held by U.S. government agencies. This pilot will assist the Department of Homeland Security (DHS) with determining whether this modality can augment existing biometric screenings for Syrian refugee applicants and also identify a threat-nexus for a subset of non-U.S. persons who attempt illegal entry. DHS is publishing this PIA because the I2B Pilot will use personally identifiable information (PII) collected from refugee applicant interviews and a subset of data from subjects apprehended at or near the U.S. border. This PIA covers the overall approach and vision for the program. This PIA will be updated if the pilot progresses to an operational state.

## Introduction

Currently, DHS and the Intelligence Community (IC) lack an integrated, interagency biometric system capability to support biometric and identity intelligence analytical tasks using unclassified and classified biometric data sources. This presents a systemic challenge to DHS efforts to identify, screen, and vet individuals who have been apprehended or who are applying for benefits. The purpose of DHS's participation in this pilot is to develop new biometric matching capabilities for immediate counterterrorism mission needs.

DHS participants include the Office of Intelligence and Analysis (I&A), U.S. Customs and Border Protection (CBP), Office of Biometric Identity Management (OBIM), and U.S. Citizenship and Immigration Services (USCIS), who are contributing data, biometric expertise, and mission user scenarios. For this Pilot, on behalf of USCIS and CBP, OBIM will provide a one-time, manual transfer of two categories of I2B Pilot records:

1. Un-adjudicated Syrian refugee applicants enrolled by USCIS for comparison to classified IC biometric holdings to assist in screening efforts for known or suspected terrorists ("Refugee Records").
2. Individuals who CBP encountered in FY2013 and determined were (1) in the United States illegally and (2) not from Mexico but whose nationality were otherwise unidentifiable for comparison to classified IC biometric holdings to assist in identification of known or suspected terrorists ("Border Records").

The I2B Pilot will: (1) evaluate identification of basic biometric capabilities and requirements for the pilot; (2) standardize biometric records to permit ingestion and matching within IC Information Technology Enterprise (IC ITE); (3) test ingestion and integration of biometric records in IC ITE and the applications to be used on the data within IC ITE; and (4) conduct mission user testing and documentation of results. DHS will provide DHS I2B pilot data for IC ITE ingestion and integration upon completion of (1) a Letter of Intent, (2) a DHS



operational concept of operations that sets forth, among other things, the specific roles and responsibilities and contemplated processes and procedures, including a description of the technical safeguards to be provided to DHS I2B Pilot data and the policy-based access rules governing the provision access to DHS I2B Pilot data; and (3) the execution of this Privacy Impact Assessment.

Although the primary intent of this pilot is to determine functional and technical requirements for a multi-modal biometrics capability (e.g., the images can be standardized and ingested successfully; the algorithms are effective), other benefits include: (1) identification of previously unidentifiable individuals related to known or suspected terrorists attempting to gain refugee status, (2) provision of actionable intelligence on individuals attempting to illegally enter the United States without valid identification, and (3) informing DHS on the effectiveness of IC-owned biometric technology. Any Terrorism Information<sup>1</sup> identified as a result of the I2B Pilot will be retained and disseminated as appropriate and applicable.

On behalf of USCIS and CBP, OBIM will send biometric file data, which includes biographic information, biometric images, and related metadata maintained in the Automated Biometric Identification System (IDENT) for the two test cases described above (i.e., Refugee Records and Border Records) to the I2B team for pilot use. Records will include biometric images (i.e., digital representation of face or fingerprint), along with available associated biographic data (e.g., name, date of birth, place of birth, height, weight, hair and eye color, gender, U.S. person indicator, alien identification number), situational information (e.g., date the biometric image was taken, reason for enrollment, identification numbers, source document description), and biometric attributes (e.g., file size, shutter speed, pixels per inch).<sup>2</sup>

An I2B User Application within IC ITE will be used to search I2B pilot data. The biometric searches will be facilitated by biometric algorithms owned by the IC. Only pre-selected, authorized users will be able to access I2B pilot data via the I2B User Application. Use of matches containing DHS data will be further limited as defined in the DHS CONOPS.

Confirmed matches constituting Terrorism Information will be retained, used, and disseminated by the IC or DHS, including updating the source systems as appropriate. For example, if a subject encountered at the border provides an alias, but a biometric match indicates

---

<sup>1</sup> Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 defines “terrorism information” as: [A]ll information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities related to--(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

<sup>2</sup> Preparation includes metadata standardization, file conversion and testing by the I2B team to evaluate data quality and conform to DHS usability, retention, and access control requirements as outlined in a forthcoming Letter of Intent (LOI).



a different name, then CBP would update the biographic record and provide the alias for existing records.

DHS's participation in the I2B Pilot will conclude no later than 180 days from the successful DHS I2B pilot data ingestion into IC ITE. At the conclusion of DHS's participation in the pilot, all DHS data and any information derived therefrom will be purged by the I2B team from the IC ITE or any other IC networks, systems, or data sets used in support of this pilot. If a person is determined to be a U.S. person with no known nexus to Terrorism Information after the initial transfer to the I2B team, any records containing that information will be identified and purged as soon as is practicable but in any event no later than five business days from the date of identification.

## **Fair Information Practice Principles (FIPPs)**

The Privacy Act of 1974 articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. Given that the Identity Intelligence Biometric (I2B) Pilot is an information sharing initiative of DHS rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This PIA examines the privacy impact of I2B sharing procedures and use of DHS biometric holdings as it relates to the Fair Information Practice Principles.

### **1. Principle of Transparency**

*Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.*

For the purposes of the I2B pilot, DHS will use biometrics records originally collected by USCIS and CBP. USCIS provides transparency regarding the collection and retention of



biometrics from persons seeking status as refugees entitled to remain in the United States through the publication of its Biometric Storage System (BSS) SORN,<sup>3</sup> its Alien, File, Index, and National File Tracking System (A-File) SORN,<sup>4</sup> and its Fraud Detection and National Security Records SORN.<sup>5</sup> DHS shares this information through OBIM (as the service provider for the DHS retention and use of its biometric holdings). OBIM provides notice of its sharing of biometrics with partners for law enforcement, national security, and counter-terrorism through the publication of the Automated Biometric Identification System (IDENT) SORN<sup>6</sup> and PIA.<sup>7</sup>

CBP has yet to provide adequate transparency of its Privacy Act-covered systems of record impacted by the pilot. CBP is required to publish a SORN for the E3 System and update the CBP Portal (E3) to ENFORCE/IDENT PIA<sup>8</sup> to cover CBP's collection and retention of biometrics from persons apprehended crossing the border at locations other than Ports of Entry (*i.e.*, lawful border crossings).

## 2. Principle of Individual Participation

*Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

For the I2B pilot, there is a risk that individuals may be unable to consent to the retention and further use of their biometrics. Refugee status is voluntary; therefore, persons may choose not to request refugee status upon seeking admission to the United States. With regard to biometrics obtained as part of an investigation for the fraudulent use of a travel document, CBP collection of biometrics is required as part of the apprehension process. Permitting an apprehended person the ability to consent to the use of their biometrics would thwart the lawful compliance and enforcement objectives of DHS's mission.

DHS provides a redress process for individuals who believe the data held on them in IDENT is inaccurate.<sup>9</sup> Individuals who believe that the data maintained about them in IDENT is

<sup>3</sup> DHS/USCIS-003 Biometric Storage System, 72 FR 17172 (Apr. 6, 2007), specifically Routine Use G.

<sup>4</sup> DHS/USCIS-001 Alien File, Index, and National File Tracking System of Records, 78 FR 69864 (November 21, 2013), specifically Routine Use EE.

<sup>5</sup> DHS/USCIS-006 Fraud Detection and National Security (FDNS) Records, 77 FR 47411 (August 8, 2012), specifically Routine Use E.

<sup>6</sup> Automated Biometric Identification System (IDENT) SORN, 72 FR 31080 (June 5, 2007), specifically Routine Use A.

<sup>7</sup> DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) PIA (December 7, 2012), *available at* [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>8</sup> DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT (July 25, 2012), *available at* [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

<sup>9</sup> For full details, see the Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), DHS/NPPD/USVISIT/PIA-002, December 7, 2012, *available at* <http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-06252013.pdf>.



inaccurate can submit a redress request for a review and correction of that inaccurate data. However, the information requested may be exempt from disclosure under the Privacy Act because these records, with respect to an individual, may sometimes contain law enforcement sensitive information. The release of law enforcement sensitive information could possibly compromise ongoing criminal investigations.

In accordance with the provisions of the Privacy Act of 1974 and Freedom of Information Act (FOIA), the procedures that allow individuals to access information in a DHS system of records are posted on the DHS public-facing website.<sup>10</sup> Individuals, regardless of citizenship, should submit redress requests online through the DHS Traveler Redress Inquiry Program (TRIP) website, [www.dhs.gov/trip](http://www.dhs.gov/trip), or mail the completed form and documents to DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 20598-6901.

### 3. Principle of Purpose Specification

*Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

The purpose of the I2B pilot is to develop a cloud-based multi-modal (face and fingerprint) automated biometric identification system using non-U.S. person biometric records held by U.S. government agencies. This pilot will assist DHS with determining whether this modality can augment existing biometric screenings for Syrian refugee applicants and also identify a threat-nexus for a subset of non-U.S. persons who attempt illegal entry. The purpose for DHS's participation in the I2B pilot is to develop new biometric matching capabilities to support biometric and identity intelligence operational and analytical tasks using unclassified and classified biometric data sources.

The pilot purposes are consistent with the original purposes of collection of the refugee and apprehension data provided by DHS to the IC, which, pursuant to the underlying source system SORNs, includes facilitating the enforcement and provision of benefits under the Immigration and Nationality Act (INA)<sup>11</sup> and related statutes.

### 4. Principle of Data Minimization

*Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

---

<sup>10</sup> [http://www.dhs.gov/xfoia/editorial\\_0579.shtm](http://www.dhs.gov/xfoia/editorial_0579.shtm).

<sup>11</sup> Authority for maintaining this information is in Sections 103 and 290 of the INA, as amended (8 U.S.C. §§ 1103 and 1360), and the regulations issued pursuant thereto; and Section 451 of the Homeland Security Act of 2002 (Pub. L. 107-296), codified at 6 U.S.C. § 271.



For the purposes of this pilot, OBIM will transmit biometric file data, biometric images, and related metadata maintained in the IDENT system for the two test cases described above to a platform maintained by the IC.<sup>12</sup> The I2B Pilot is designed to exclude any information pertaining to U.S. citizens, lawful permanent residents, and individuals with protections under 8 U.S.C. § 1367. DHS has required that there must be an ability to identify and immediately purge all records for any person whose status changes to U.S. person. Disclosure of records will be tracked. The I2B Letter of Intent between DHS and the IC documents the authorization to share the IDENT information to DHS's IC partners for the purposes of the I2B Pilot. DHS oversight offices, including the Office of Policy (PLCY), the Privacy Office (PRIV), the Office for Civil Rights and Civil Liberties (CRCL), and the Office of the General Counsel (OGC), will oversee the pilot to verify the data's use.

Because the data that DHS will provide to the I2B Pilot is stored in IDENT, the I2B Pilot will inherit the accuracy risks identified in the IDENT PIA and rely upon the associated mitigations.<sup>13</sup> The I2B Pilot will also inherit the accuracy risks from the other contributing Partners' systems. To mitigate the accuracy risks that come from combining data from multiple systems, the I2B Pilot will rely on human review by trained DHS biometric experts to confirm any matches between the DHS provided data and previously unknown terrorism information. Moreover, DHS will require that a trained DHS analyst verify any match based on information provided by DHS.

## 5. Principle of Use Limitation

*Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

DHS's participation in the I2B Pilot will conclude no later than 180 days from successful DHS I2B pilot data ingestion into IC ITE. At the conclusion of DHS's participation in the pilot, all DHS data and any information derived therefrom will be purged by the I2B team from the IC

---

<sup>12</sup> Records will include biometric images (i.e., digital representation of face or fingerprint), along with available associated biographic data (e.g., name, date of birth, place of birth, height, weight, hair and eye color, gender, U.S. person indicator, alien identification number), situational information (e.g., date the biometric image was taken, reason for enrollment, identification numbers, source document description), and biometric attributes (e.g., file size, shutter speed, pixels per inch). Data elements include: Fingerprint Identification Number (FIN), Encounter Identification Number (EIN), facial image, and fingerprint image. The biometric data will come from the following two OUS (Organization, Unit, Subunit): DHS02 – CBP/USBP and DHS48 – USCIS/Refugee.

<sup>13</sup> For example, the IDENT PIA discusses how, a limited number of instances, the automated biometric match process will result in biometric information that does not correctly map to one individual. This can occur, for example, when an individual has low quality fingerprints, which increases the likelihood of a matching error and causes the system to establish two identities for one person. For full details, see the Privacy Impact Assessment for the Automated Biometric Identification System (IDENT), DHS/NPPD/USVISIT/PIA-002, December 7, 2012, available at <http://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-06252013.pdf>.



ITE or any other IC networks, systems, or data sets used in support of this pilot. If a person is determined to be a U.S. person with no known nexus to Terrorism Information after the initial transfer to the I2B team, any records containing that information will be identified and purged as soon as is practicable but in any event no later than five business days from the date of identification. Access to DHS I2B records will be limited, and DHS will further confirm legitimate use prior to sharing outside the Department.

The uses of the DHS data in the I2B Pilot are consistent with the original purposes of collection, which includes facilitating the enforcement and provision of benefits under the INA and related statutes. Confirmed matches constituting Terrorism Information will be retained, used, and disseminated by the IC or DHS, including updating the source systems as appropriate.

## 6. Principle of Data Quality and Integrity

*Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

The I2B Pilot does not change the initial collection of the information that takes place either directly from the individual or at the request of the individual. There is a risk that the quality and integrity of information that will be collected and maintained in IDENT may not meet the standards required to serve its purpose of biometric and biographic verification and matching, thus potentially causing misidentification. Because OBIM does not collect the information provided, the processing and storage of data in IDENT is dependent on the appropriate and accurate data fields of incoming records, which have been identified to correspond with IDENT data fields. IDENT performs certain quality checks (e.g., determining the quality of a captured fingerprint and its suitability for matching in the future) and seeks to ensure that the data meets a minimum level of quality and completeness. However, it is ultimately the responsibility of the original data owner, whether an organization external or internal to DHS, to ensure the accuracy, completeness, and quality of the data.

All DHS data ingested for the I2B Pilot has been obtained for purposes that are consistent with DHS authorities. An individual's opportunities to seek redress would rely on those of the IDENT system, and would apply to the I2B Pilot.

## 7. Principle of Security

*Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

DHS, through the published SORNs and PIAs for USCIS's BSS, A-File, and FDNS systems and OBIM's IDENT system has documented the security requirements and practices employed to protect and safeguard the DHS biometrics used for this Pilot. In addition, the LOI between DHS and the IC, used to govern the exchange of information to facilitate the Pilot, sets



forth additional requirements concerning user access provisions, use limitations, and data integrity checks to ensure that only verified biometric matches to terrorist information are shared and retained for further use. Lastly, the IC partners' recipient systems comply with Intelligence Community Directive 503 (Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation).

## **8. Principle of Accountability and Auditing**

*Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

Multiple DHS offices—including CRCL, I&A, OGC, PLCY, and PRIV—will participate in a review to evaluate the I2B Pilot upon completion. DHS, acting in coordination with I2B participants, will document the results of this evaluation.

## **Responsible Officials**

Benjamin Stefano  
Senior Advisor  
Office of Intelligence and Analysis  
Department of Homeland Security

## **Approval Signature Page**

Original signed copy on file with the DHS Privacy Office

Karen L. Neuman  
Chief Privacy Officer  
Department of Homeland Security