Homeland Security

DHS International Biometric Information Sharing (IBIS) Program

Enhanced Biometric Security Partnership (EBSP)

The IBIS Program provides foreign partners and DHS Components with a scalable, reliable, and rapid bilateral biometric and biographic information sharing capability to support border security and immigration vetting. IBIS creates value for the United States and its partners by detecting fraud, identifying transnational criminals, sex offenders who have been removed from the United States, smugglers of humans and narcotics, gang members, terrorists and terrorist-related information, and the travel patterns of criminals.

Every IBIS partnership begins with cooperation under a negotiated Enhanced Border Security Agreement (EBSA) or a similar legal instrument. The EBSA provides a flexible but enduring framework to facilitate information exchange for criminal, border and national security, immigration, and counterterrorism purposes at high volumes (up to millions of transactions each year) without requiring manual intervention for each disclosure. The EBSA outlines specific expectations for appropriate handling and protection of personal data exchanged.

Under the negotiated legal framework, IBIS partners may submit biometrics to DHS to search against the entire IDENT/HART repository to identify matches to U.S. holdings using a secure encrypted gateway called the Secure Real Time Platform (SRTP). IDENT/HART is the largest U.S. Government biometric database and the second largest biometric database in the world, containing over 270 million identities from over 40 U.S. agencies. In the event of a match to a record in IDENT/HART, DHS can immediately provide available and sharable associated biometric, biographic, derogatory, and other encounter information to the partners. These responses help foreign partners determine or validate the identity of individuals they encounter, detect fraud and immediately identify public security threats. Where necessary, DHS supports further information exchange and operational cooperation through an extensive network of attachés located at U.S. Embassies and diplomatic posts.

In turn, DHS may submit biometrics to IBIS partner countries to search against their biometric identity management systems in order for partner countries to provide DHS with sharable biographic, derogatory, and encounter information when a U.S. search matches their biometric records. This high-volume matching and data exchange is accomplished within minutes and is fully automated; match confirmation and supporting data is exchanged with no officer intervention. This bilateral information sharing protects public safety and strengthens the public security of both the partner country and the United States.

DHS recognizes each partner has a diverse range of technical capabilities, unique institutional structures with differing data owners and domestic databases. DHS works closely with the foreign partner to customize the IBIS Program and also has a flexible IT architecture that gives countries multiple ways to implement the capability based on those unique requirements and capabilities.

Benefits

- Near Real-Time Biometric Matching to U.S. Data Fraud and Criminal Detection
- Identification of Smuggling Trends, Actors, and Pathways
- Alerts for Known Fugitives, Terrorists, and Criminal Actors
- Identification and Protection of Trafficking Victims
- Enhanced Capacity to Share Information Across Ministries and Agencies
- Intuitive and Actionable Responses
- Possible Integration with Other U.S. Programs
- Enables Local Operational Cooperation to Mitigate Public Safety Threats
- Advanced Data Analysis

Homeland Security

Potential U.S. Data Available to IBIS Partners

As the largest federal law enforcement agency in the United States, DHS maintains unique data that is valuable to IBIS partners for detecting and identifying fraud, criminal activity, and investigative leads.

For example, ICE and CBP investigate and have large volumes of information on individuals engaged in cross-border and transnational crime, such as illicit drug and human trafficking, including by U.S. persons.

IDENT/HART includes records from the U.S. Departments of State, Justice, and Defense, and state and local law enforcement entities.

Upon a biometric match, DHS makes as much data automatically available to partners as possible consistent with legal, privacy, and policy limitations.

After a fingerprint match, IBIS partners may have near real-time automated access to information contained in IDENT from DHS and other U.S. agencies regarding persons:

- Who are known or suspected terrorists
- Arrested by Federal or State authorities and deported for criminal offenses
- Investigated or convicted and deported for transnational crimes, including human and narcotics trafficking
- Ordered removed from the U.S. and/or found in violation of U.S. immigration law
- Convicted of a felony and subsequently deported from the U.S.
- Identified by DHS as a member of a gang
- Identified by DHS as human traffickers or smugglers
- Identified by DHS as narcotics traffickers or smugglers
- Apprehended by DHS law enforcement officers
- Encountered by the U.S. military in combat zones
- With other public security and criminal history alerts
- Arrested for entering the U.S. without authorization, and persons overstaying their visa
- Applying for and/or denied visas to travel to the U.S.
- Arriving at ports of entry to the U.S., including adverse actions taken at secondary examinations during previous arrivals
- Applying for most immigration benefits in the U.S.
- Who applied for asylum or refugee status in the U.S.
- Applying for select government work credentials

IDENT contains over 1.1 billion "encounters," each of which consists of a distinct biometric collection by a U.S. government agency on a specific date and time for a particular purpose. Each of the approximately 270 million unique identities may have multiple "encounters" associated with it, and DHS is able to share information on each separate encounter when there is a biometric match to the identity, consistent with policy and legal requirements.

Each individual encounter may include the following:

- *Biometric Data:* fingerprints, digital facial photographs, scars, tattoos, marks, and iris images
- *Personal Information:* full name (i.e., first, middle, last, nicknames, and aliases), date of birth; gender; personal identifiers including a fingerprint identification number and an encounter identification number; citizenship and nationality, and country of birth; passport and visa data; document type; other document types; document number, and country of issuance
- *Encounter Data:* contextual information about the nature of U.S. interactions, including transaction-identifier data such as the sending organization; timestamp; reason sent (e.g. entry, visa application, credentialing application, or apprehension); and any available encounter information
- *Derogatory Information*: a code describing the nature of the derogatory information associated with an identity is provided n the real time response, enabling officers to quickly understand important contextual information without needing to reference or interpret U.S. law. DHS currently may be able to make available the following derogatory information to partners where authorized by law, policy and international instruments:
  - Known or suspected terrorists (KSTs)
  - Sexual offender removals
  - Some federal conviction information, where available
  - Criminal convictions for immigration and cross-border crimes
  - Immigration violations and revoked visas
  - Military records
  - Criminal history information pertaining to aliens removed from the U.S.
  - Known or suspected gang members
  - Known or suspected drug smugglers
  - Known or suspected human traffickers or human smugglers
  - Law enforcement community alerts