



Fact Sheet

IDENT and IAFIS Interoperability

Goal of IDENT and IAFIS Interoperability

As a part of the U.S. government's efforts to enhance our nation's security to meet the needs and challenges of the 21st century, the Department of Homeland Security (DHS) and Department of Justice/Federal Bureau of Investigation (DOJ/FBI) will continue to improve their technological capabilities to provide access for information sharing among immigration, law enforcement and authorized non-criminal justice agency officials, such as Office of Personnel Management (OPM), about known or suspected terrorists, criminals and immigration violators.

As a part of these improvements, DHS and DOJ/FBI are working to establish interoperability between the US-VISIT program's Automated Biometric Identification System (IDENT) and the FBI's Integrated Automated Fingerprint Identification System (IAFIS) fingerprint databases.

The goal of IDENT and IAFIS interoperability is to allow the real-time exchange of biometric and biographic information between agencies that is complete, accurate and timely. Interoperability will ensure that federal, state and local law enforcement, authorized non-criminal justice agencies and immigration officials will have better information with which they can use to make decisions.

What are IDENT and IAFIS?

IDENT is a DHS database that contains the biometric information of international travelers to the United States who are enrolled through DHS's US-VISIT program, as well as known or suspected terrorists, criminals, immigration violators and others. IDENT is currently based on a two-fingerprint, digital collection system for identity establishment and verification purposes. The program is transitioning to collect 10 fingerprints in the future.

IAFIS is DOJ/FBI's biometric database and it is maintained by the DOJ/FBI's Criminal Justice Information Services (CJIS) division. The IAFIS is a 10-rolled fingerprint identification system that was deployed in 1999 and is used by federal, state and local law enforcement and authorized non-criminal justice agencies to identify subjects with criminal history information.

Achieving Interoperability

In September 2006, DHS and DOJ/FBI made technology enhancements to these databases, which provided immediate tangible benefits to federal, state and local law enforcement, non-criminal justice agencies, as well as consular officers and immigration officials. These technology enhancements represent the first in a series of three phases to achieve full interoperability of IDENT and IAFIS: an interim solution, initial operating capability (IOC) and full operating capability (FOC). The first phase consists of a pilot program, known as the interim data sharing model (iDSM). These technology enhancements will further improve fingerprint-based access and sharing of criminal history information among immigration officials and will, for the first time, allow fingerprint-based access to immigration history information to state and local law enforcement and an authorized non-criminal justice agency.

During the second phase of enhancements called IOC, DHS and DOJ/FBI plan to expand the categories of data shared and further enhance the infrastructure for data exchange and search capabilities between these two databases. During this phase, DHS' US-VISIT program will move from collecting two fingerprints to collecting 10 fingerprints, which will increase accuracy in identity verification and will complement the IAFIS database, which is based on 10 fingerprints.

DHS and DOJ/FBI plan to implement the third phase for achieving database interoperability, FOC, which will provide additional data and further automate many of the processes.

Current Capabilities

Today, biographic information linked to biometrics about criminals or immigration violators within both databases is accessible and exchanged as required and authorized by immigration and law enforcement officials. Biographic information may refer to names used, date of birth, criminal history record information, travel history, civil or immigration status, etc. Biometric information refers to a measurable biological or behavioral characteristic used for identification—a digital photograph or fingerprint.

In September 2006, DHS and DOJ/FBI launched a new process, iDSM, which allows for two-way sharing of biometric and biographic information, including all IAFIS wants and warrants, expedited removals and visa applicants that the Department of State (DOS) has determined to be a substantial risk to enter the country and has denied their application for a visa (Category One visa refusals).

DHS and DOJ/FBI selected three agencies to pilot iDSM, the first phase of interoperability: the Boston Police Department; the Dallas County Sheriff's Department; and the OPM.

During the pilot, federal, state and local law enforcement and authorized non-criminal justice agencies, will have fingerprint-based access to immigration history information, and U.S. immigration officials will have fingerprint-based access to criminal history information in real time to make timelier and more informed decisions.

With the technology enhancements, Immigration and Customs Enforcement's (ICE) Law Enforcement Support Center will evaluate the immigration information when fingerprints match those of someone who was denied a visa or required expedited removal and notify the local ICE office to take appropriate action. The official requesting the information will receive automatic notification from DOJ/FBI once ICE has responded back with the evaluated immigration information. Previously, state and local law enforcement were required to contact ICE separately to inform them of a match.

Additionally, DHS and DOJ/FBI will add or remove information about a subject as it changes, like a new expedited removal charge or a cancelled want notice. DHS and DOJ/FBI will communicate such changes through an automated process, making such information available more quickly.

See Diagram A for a visual explanation of the new process—iDSM.

Move to 10 Fingerprints

In addition to DHS and DOJ/FBI working toward IDENT and IAFIS interoperability, US-VISIT is transitioning from the collection of two fingerprints to the collection of 10 fingerprints. In 2008, US-VISIT plans to begin collecting 10 fingerprints from travelers at ports of entry to coincide with the completion of the second phase of interoperability, IOC.

Moving to a 10-fingerprint standard will enable DHS and DOS to identify travelers or visa applicants with even greater accuracy than we do today, send fewer people to secondary inspection, allow border and visa-issuing officers to focus more on those who might be greater risks and will complement the IAFIS database, which is based on 10 fingerprints.

Respecting Privacy and Environment

DHS and DOJ conducted a Privacy Impact Assessment for the iDSM, and all information exchanges comply with the Privacy Act and existing privacy policies.

The IDENT data, which is stored by FBI/CJIS, is secured in accordance with the DHS and DOJ/FBI information system security procedures. IDENT data shared with FBI/CJIS users (Boston, Dallas and OPM) is secured according to the protection regimen established by each user.

What are US-VISIT and CJIS?

US-VISIT is one of DHS's most notable successes and its establishment of biometric entry capabilities at 117 airports, 16 seaports and 154 land ports of entry are key to the implementation of our country's immigration and border management strategy. US-VISIT has evolved into an organization that provides identity services for most operational components of DHS, and assists other government agencies through the appropriate collection and sharing of biometrics.

The Criminal Justice Information Services Division (CJIS) serves as the focal point and central repository for criminal justice information services in the FBI. CJIS is a customer-driven organization that provides state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities.

Diagram A: iDSM New Process Graphic

