LEDS/HOB Open Space:

Home Office Biometrics (HOB) Programme

Granular Detail of HOB systems

[v1.0, 09/04/19]

Discussion Document

Following the discussion at the February workshop, this document provides Open Space with further details of the HOB systems – data inputs, HOB systems connections and details of the uses. The purpose of the paper is to give Open Space more granularity of the HOB Programme and systems upon which future Open Space sessions can be designed on the areas of most interest to participants

It is not intended to be viewed as current Home Office policy or intention. It is to be circulated to and viewed only by members of the LEDS/HOB Open Space.

Purpose

Following the discussion at the February workshop, this document provides Open Space with further details of the HOB systems – data inputs, HOB systems connections and details of the uses.

This paper will be issued with the agenda for the Open Space workshop on 14th May 2019 and will aim to:

- Provide Open Space with more granularity of the HOB Programme and systems
- Invite the views from Open Space participants on the areas of most interest to them upon which future sessions can be designed

Summary

At the Open Space workshop in February Home Office Biometrics gave a presentation detailing the main elements that make up the programme. The subsequent discussion with Open Space Participants highlighted a number of themes and areas for future discussion including interactions between different users (e.g. law enforcement and immigration) and a map of HOB & other biometrics programmes (how they fit together, along with local forces, etc).

The following paper provides more detailed information on the HOB systems, links through to a legislative summary information and provides further details on the future Strategic Matcher Platform and logical separation of data.

We will be bringing the full set of theme and issues, and others as they arise within the programme, to the Open Space at an appropriate time and are happy to discuss priorities if participants are interested in doing so.

Home Office Biometrics (HOB) Programme granular detail of HOB systems

HOB Recap

1. The HOB Programme has a responsibility to provide biometrics related services to a wide range of Home Office and government users. This is currently Departments and agencies involved in immigration and law enforcement and the full list is outlined below.

2. The systems in scope in the HOB Programme that provide such biometric services are:

   - **IDENT1 (Law Enforcement and Security Biometrics System)** – provides biometric enrolment, identification and identity management services within the law enforcement domain, principally for arrestees in the UK, but also covering other specialist data sets.
   - **Immigration and Asylum Biometrics System (IABS)** – provides biometric enrolment, identification, identity management and verification services within the immigration and citizenship domains. E.g. for visa applicants to the UK, biometric residency permit applicants, asylum applicants and passport applicants.
   - **National DNA Database (NDNAD)** – the NDNAD holds DNA profiles of subjects in criminal cases, some of whom have not been convicted of a crime and profiles of victims, as well as marks from crime scenes. The database also holds DNA profiles of vulnerable persons who fear they may be victims of a crime; volunteers who may be vulnerable to attack themselves if their details become known to the wider public; and police officers for elimination purposes. The missing persons and the contamination elimination databases are currently held on a different infrastructure. However, it is planned that the strategic DNA Service will store all data in a single database made up of multiple, logically separated collections.
   - **Biometric Accuracy Test (BAT) environment** – through the Biometric Accuracy Testing (BAT) environment, HOB has undertaken a full and comprehensive approach to testing to select the most advantageous matcher software, and to provide wider assurances of future biometric capabilities

HOB system connections

IABS		
Inputs	**Connected to**	**Types of usage**
• UKVI collect fingerprints and facial images from foreign nationals applying for visas, asylum or residence in the UK. • HM Passport Office (HMPO) collect facial images as part of the passport application process	• Foreign & Commonwealth Office Services (FCOS) and supporting UK Visas & Immigration (UKVI) services - visas etc. • Home Office Immigration; Border Force, UKVI & Immigration, Compliance & Engagement (ICE) • Immigration Platform Technologies (for Biometric Resident Permits) • HM Passport Office • Policing • International Data Sharing Capability (now called Migration 5) • EURODAC	Checks against biometric records to: • confirm identity • application management and issuing case outcome • Identify previous applications • Latent mark searching to identify links to crime scenes

	• IVACs (Irish Visas)	

IDENT1		
Inputs	**Connected to**	**Types of usage**

The police collect fingerprints from arrestees in police custody suites. IDENT1 also contains elimination & missing person data which is collected with consent	• All police forces in England, Wales, Northern Ireland & Scotland
	• Specialist bureaux within law enforcement and government agencies including:
	  ○ National Fingerprint Office (NFO)
	  ○ Counter Terrorist Forensic Service (CTFS),
	  ○ International Law Enforcement (via requests made to the National Crime Agency)
	  ○ Ministry of Defence (MoD)
	  ○ National Crime Agency (NCA)
	  ○ HM Revenue & Customs (HMRC)
	  ○ IDENT1 Training Suites
	• Government agencies and Crown dependencies which do not have their own bureau have made arrangements to use a specific force's bureau. These include:
	  ○ Department for Work & Pensions (DWP)
	  ○ Royal Mail Investigations
	  ○ RAF Police
	  ○ Isle of Man
	  ○ Jersey
	  ○ Guernsey
	• ACRO Criminal Records Office
		Checks against biometric records to:
		• confirm identity
		• Identify previous arrests
		• Eliminate individuals from a crime scene
		• Identify missing persons
		• Latent mark searching to identify links to crime scenes

BAT Environment		
Inputs	**Connected to**	**Types of usage**
Sample data collections from IABS and IDENT1 provided with the agreement of the Information Asset Owner	• Standalone system	Checks against biometric records to: • Test supplier algorithms as part of procurement • Evaluate the accuracy of algorithms

HOB legislation

A full legislative summary has been published on GOV.UK. The documents contain details of the permitted uses and retention periods for biometric data held on IABS and IDENT1. Biometric information held on the BAT environment is covered by the specific retention periods outlined in the data sharing agreement and also legislative requirements.

The published documents are currently under review along with other HOB Privacy Impact Assessment documents.

Future Strategic Matcher and logical separation

While all biometric records, whether it is a fingerprint or facial image, will use the Strategic Matcher platform, they are organised according to the purpose for which they were captured (e.g. HMPO passport facial image, immigration fingerprint). This is how the data remains logically separated – the Strategic Matcher platform will not mix biometrics from different purposes within a single record. There will be reconciliation mechanisms in the Strategic Matcher that will be run continuously to assure there is no mix up of data and logical separation will be assured through a mature testing approach.

The matcher software, which will run on a separate platform to the biometric databases, is used in a number of situations to search the IABS or IDENT1 databases, such as:

- the police verifying the identity of an arrestee,
- the police identifying an individual from fingerprints found at a crime scene
- the police verifying the identity of a suspect using the mobile biometric application in the field
- Border Force officers verifying the identity of someone entering the UK on a visa at the point of entry
- Immigration Enforcement officers verifying the identity of someone who has entered the UK on a visa
- Immigration Enforcement officers verifying the identity of a suspected immigration offender using the mobile biometric application in the field

The new matcher platform and matching algorithms will not give agencies access to any new data. Clear business rules are to be built into the workflow of the Strategic Matcher platform to manage the matching requests and each new business rule must be individually authorised prior to implementation so that matching requests are made against the relevant data sets only. There is a process that is followed for each proposed new business rule involving Business & Technical Design Authorities and Live Service Change Management. Further approvals that may also be required from the operation business area or regulators and this is identified as each business rule is designed.