Home Office

Home Office Biometrics Programme

Privacy Impact Assessment

Version 1.5

This PIA was agreed on 2nd May 2018

Contents

Executive Summary

1. The Home Office Biometrics (HOB) Programme is a Government Major Projects Portfolio (GMPP) programme of strategic significance across Government which commenced in 2014 and will finish in 2020/21.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

2. The current HOB Programme is focussed on maximising the public safety benefits of fingerprints, DNA and facial matching. With biometric technology developing at pace, and with new biometrics emerging rapidly, this landscape brings with it a number of important choices for Government, especially how to maximise the potential benefits to the public whilst protecting the privacy of the individual and addressing any potential impact of data aggregation.
3. The HOB Programme will transform the existing siloed biometrics capabilities into a technically converged, but commercially disaggregated, strategic biometrics capability. This new capability will be delivered through a number of projects which are outlined later in this document.
4. Privacy Impact Assessments (PIA) have either been completed or are underway for all of the HOB projects. HOB is also committed to undertaking an ethical review of the projects and all PIAs are considered by the HOB Ethics Working Group during their development. Together they accumulate to form the Programme PIA which is the focus of this document. It covers the following areas:

   a. Section 1 introduces the HOB Programme, the key delivery objectives and the main projects that make up the Programme.

   b. Section 2 outlines why the HOB Programme believes it is important that a Privacy Impact Assessment be undertaken and how the Programme has conducted this assessment.

   c. Section 3 details the methodology employed, including consulting and engaging with stakeholders.

d. Section 4 outlines the main areas of privacy concern that have been identified and will be addressed by the HOB Programme

e. Section 5 outlines how the Programme will undertake an ongoing review, audit and updating of the PIA.

f. Annex A provides brief descriptions of the main biometric databases.

g. Annex B details the initial screening process which was undertaken to consider the requirement for a PIA. (The screening questionnaire is published separately)

h. Annex C provides a table of the relevant legislation for biometric capture, usage and retention.

i. Annex D outlines the individual PIA for each of the main projects within the HOB Programme. (For publication only the status table of project PIAs will be included in this document. Individual project PIAs will be published separately because it is likely that they will be reviewed and updated at different times, and new DPIAs will be added to the suite of HOB Programme PIA/DPIAs)

j. Annex E lists the organisations who the HOB Programme team have consulted during the PIA process.

k. Annex F considers compliance with the data protection legislation and other relevant legislation (The legislation summaries are published separately).

l. Annex G provides a glossary of terms

Section 1: The Home Office Biometrics (HOB) Programme

HOB Programme overview

1.1 The HOB Programme is delivering services supporting fingerprints, facial images and DNA (the main biometric modalities currently extensively used in the UK public sector), developing capabilities across the Home Office, law enforcement and, where appropriate, more widely across government. HOB will facilitate greater efficiency in the way that biometric services are delivered to users in the wider Public Sector.

1.2 The use of biometric technology to identify and verify individuals is already well established and used extensively by police forces, the National Crime Agency (NCA), within the Home Office including HM Passport Office (HMPO), Border Force, UK Visas & Immigration (UKVI) and other by Government Departments, for example the Ministry of Defence. It is therefore a critical element of our national security and public safety infrastructure.

1.3 The current HOB Programme focusses on maximising the public safety benefits of fingerprints, DNA and facial matching. With biometric technology developing at pace, and with new biometrics emerging rapidly, this landscape brings with it a number of important choices for Government, especially how to maximise the potential benefits to the public, whilst protecting the privacy of the individual and addressing any potential impact of data aggregation. While all the collections of biometric data will be physically in one system they will be logically separated with role-based access controls (RBAC) allowing user access only to the data and activities they are permitted to access.

The logical separation of data, supported by strong governance around the management of the data, is an important step in the evolution of the biometric systems for immigration and law enforcement, and in meeting the objectives of the HOB Programme. The development of the governance in the Home Office will continue to be an important element of the HOB Programme, alongside the technical developments.

1.4 The Home Office has existing biometrics systems with contracts that come to an end in 2019. HOB aims to evolve these systems to provide continuity beyond 2019 and enhance their capability through a number of phases. The three primary objectives of the Programme are as follows:

- Business Continuity – continuity of current biometric capabilities provided by existing contracts and services (IDENT1, IABS and NDNAD – descriptions of these three main biometric databases are found below and in Annex A);
- Cost savings – reductions in operational costs, when compared to a like for like basis at the start of the programme;
- Enhanced biometrics capability.

1.5 The HOB focus in 2017/18 through to 2020/21 is the delivery of biometric services, including matching biometrics against existing collections, and new or enhanced biometric capabilities, such as front end equipment or applications, thereby supporting and enhancing the operational effectiveness of the service users.

HOB Programme detail

The HOB Programme has a responsibility to provide biometrics related services to a wide range of Home Office and government users. Fundamental to providing these services will be a flexible and comprehensive biometric IT platform. The platform will support different user groups, data sets, biometric modalities and stakeholder requirements.

1.6 The biometric platform, referred to as the HOB “Biometric Services Platform” (BSP), is made up of the back-end elements that provide the biometric services (search, verify, enrol, etc.) and the complementary front end equipment in the form of mobile biometric and enrolment capture capabilities.

1.7 There are a number of IT systems already in scope in the HOB Programme that provide such biometric services, but they do so in a siloed way. Brief outlines of the three main IT systems are below with fuller descriptions in Annex A:

- 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

1.8 The HOB Programme will transform the existing siloed biometrics capabilities into a technically converged, but commercially disaggregated, strategic capability. This new capability will be delivered through a number of projects which are outlined below. It should be noted however that the new DNA system is unlikely to move onto the strategic biometric platform in the lifetime of the programme.

1.9 Where it is considered appropriate for a strategic project to undergo a privacy assessment, a PIA will be duly completed. The project PIAs, briefly described here and attached in full at Annex C, cumulatively form the HOB programme PIA.

1.10 The HOB biometric services platform delivery scope covers:

- Biometric Services Core[1], which includes the main service-providing back end subsystems such as the Biometric Services Gateway (BSG), Central & Bureau and Matcher sub-systems.
- Front End Equipment[2] and Mobile capability. Note that the platform also supports enrolment capture capability being provided by third parties and in such cases it includes the provision of Application Programme Interfaces (APIs), which are a clearly defined set of protocols enabling different

[1] PIAs applicable for Biometric Services Core are Biometric Services Gateway, Central & Platform, Matcher & Bureau Services.

[2] The current PIAs for Front End Equipment are Strategic Mobile and the Livescan Pilot

technologies to work together, with associated security, communication channels, standards, audit, and quality assessment services.

1.11 The sub-systems making up the Biometric Services Core and the Front End Equipment elements are shown in Figure 1 below.

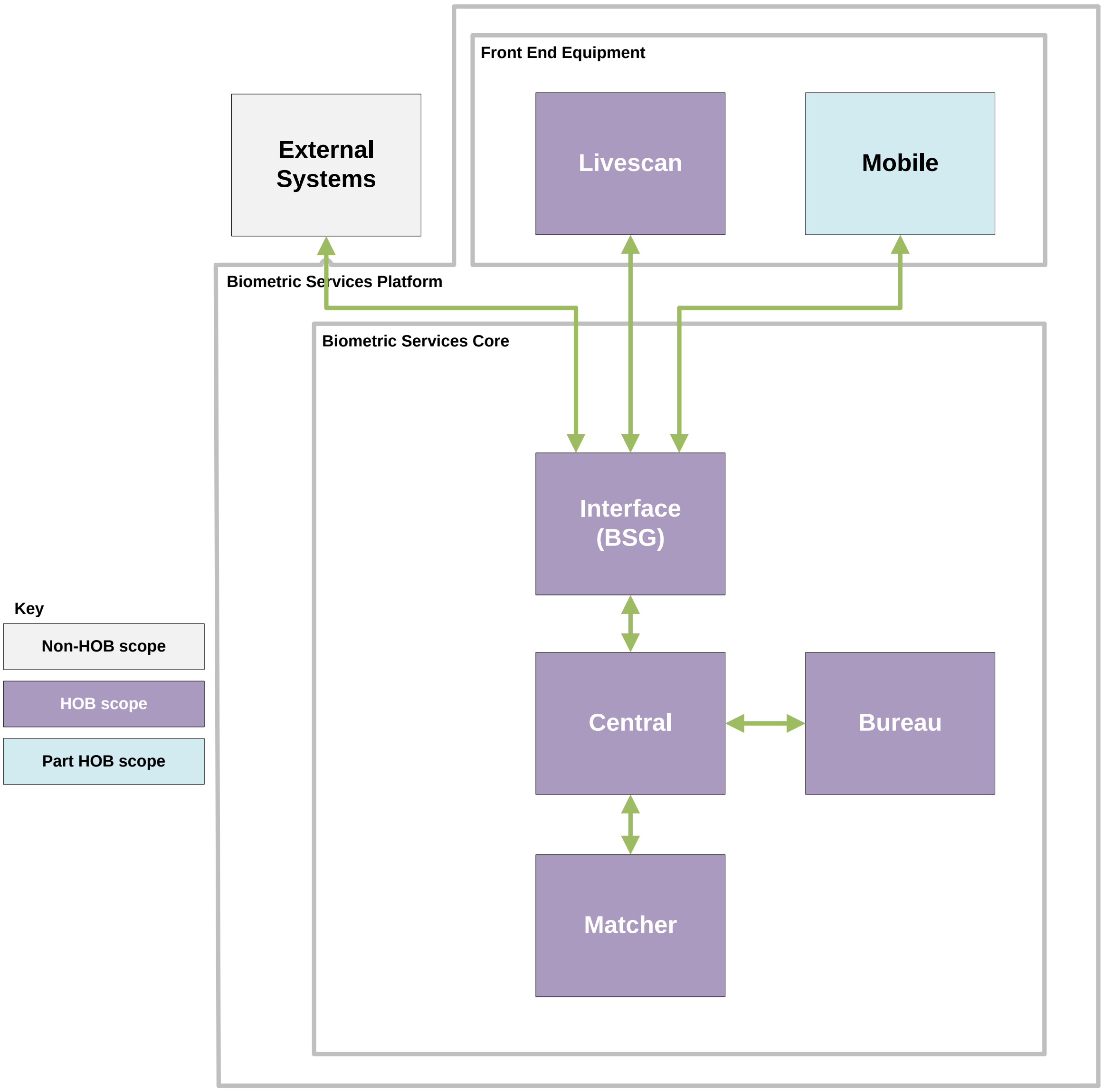

Figure 1 - HOB Scope and Biometric Services Platform

1.12 Brief descriptions of the projects within the scope of the HOB Programme are as follows:

- **Biometric Services Gateway (BSG):** The universal 'front door' to HOB services.

  - Reduces the complexity of the IT environment by introducing standards and common formats.
  - Reduces the future cost of integration between HOB and other systems/services.
  - Reduces ongoing run costs and increases system robustness and resilience.

  The BSG phase 1 went live in January 2017, phase 2 in June 2017[3].

- **Strategic Matcher:** The HOB Strategic Matcher project will provide a Biometric Matching Service delivering biometric search, identification and verification capabilities across multiple biometric modalities (initially fingerprints and face) and for multiple data sets (immigration, citizenship, law enforcement, etc). The first algorithm will be a new matching capability for law enforcement for fingerprints which will enhance that capability, making matching faster and more accurate. The service has been procured and contracts awarded. The new system will be live in late spring 2019.
- **Strategic Central & Bureau Project:**
  - Creation of a new HOB central platform which is at the heart of the strategic Biometric Service. This Central platform is the location of the key biometric data stores and also workflow which orchestrates all the other sub-systems.
  - While all the collections of data will be physically in one system they will however be logically separated with role-based access controls (RBAC) allowing user access only to the data and activities they are permitted to access.
  - The bureau platform is part of the same project and provides a platform onto which the bureau tools and applications will be deployed.
  - There is an active procurement underway for the SCBP

[3] BSG PIA provides further explanation of the deliverables in each phase – which removed Departmental Infrastructure Service Boxes (DIS boxes) and replaced them with a biometric services gateway

- **Strategic Front End Equipment (FEE)** will provide front end equipment for the capture and verification of biometric data. This project has deployed new Livescan3 machines, replacing Livescan1 and 2 machines, used in police custody suites across the UK.
- **Strategic Mobile** will enable Police and Immigration to access Law Enforcement and Immigration biometric services from mobile devices as a data service consumed within operational mobile applications. The replacement for the current police capability was driven by the end date of the existing contract. It will subsequently be rolled out to Immigration Enforcement and Borders.
    - This marks a new approach for HOB as, instead of HOB providing the devices, Police Forces determine which mobile device to use. Forces may put the apps onto existing mobile devices. There is also the need to have a biometric peripheral for capturing the prints.
    - This will allow users to search a fingerprint provided by a suspect against both immigration and crime fingerprint databases and in both cases will speed up identification and triage of suspects and offenders, i.e. where an officer can identify who an individual who is suspected of committing an offence and providing false information about their identity through a mobile search on the street, they can in some instances avoid having to make an arrest just to confirm identity back at the custody suite - fingerprints can be taken in the field from a non-arrested person without consent only if these conditions apply. Biometric data is not recorded or stored as a result of being captured through a mobile device.

1.13 There are also other projects that come within the scope of the HOB Programme but do not directly fit within the BSP and these are also outlined below.

- **Strategic DNA** This project, to be delivered in 2019, will provide a secure, accredited and legislatively compliant profile storage, search and matching facility to replace the existing database. It will maintain current capabilities and the functionality available to the user today. The solution will also deliver full, end-to-end automation for routine transactions, ensuring a more responsive service and delivering business efficiency. The Strategic DNA project will also improve resilience of the platform and, in addition to future-proofing the solution, will provide a flexibility that supports customer process change, with a data model and components that are customisable. The new system is unlikely to move onto the strategic biometric platform in the lifetime of the programme.

- **International data sharing.** HOB is delivering part of the UK's commitments to the **Prüm Council Decisions**[4] [5], specifically Prüm Fingerprints – sharing fingerprint records with EU nations for the purpose of law enforcement and counter terrorism. Prüm DNA, which will see DNA records shared with EU partners, is being delivered in partnership with the Metropolitan Police Service, adapting and reusing the solution which has been piloted.
- **Strategic Facial Matching for Law Enforcement** was accepted into the HOB scope in March 2017. The project will deliver a new algorithm with storage and retrieval for law enforcement facial image matching, ensuring continuity of the current Police National Database (PND) face functionality.

[4] COUNCIL DECISION 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. http://ec.europa.eu/dgs/olaf/data/doc/2008-615.pdf

[5] COUNCIL DECISION 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF

Section 2: Privacy Impact Assessments[6]

Information Commissioners Office (ICO) guidance on PIAs

2.1 The Privacy Impact Assessment (PIA) handbook issued by the Office of the Information Commissioner in 2007 recommended PIAs as good practice for any initiative involving new or significant changes to the processing of personal information. This was followed in February 2014 by the Conducting Privacy Impact Assessments Code of Practice, published by the Information Commissioners Office (ICO) with updated guidance on how to conduct a PIA.

2.2 The Information Commissioner suggests in the Code of Practice, the type of project which might require a PIA including:

– *“A new IT system for storing and accessing data.”*

– “*A data sharing initiative where two or more organisations seek to pool or link sets of personal data.”*

– *“Using existing data for a new or unexpected or more intrusive purpose”,* and

– *“A new database which consolidates information held by separate parts of an organisation”*

2.3 In further guidance provided in 2014[7], the ICO made it clear that it is essential for organisations involved in the processing of personal data to be able to determine whether they are acting as a controller or as a processor[8], with the following definitions:

- “data controller” means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed

[6] Under the new data protection regime from May 2018, PIAs will be known as data protection impact assessments (DPIAs) and it will be mandatory for a controller with technologies such as those described in this document. The latest ICO guidance is https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[7] https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

[8] In the new data protection regime, post 25 May 2018, the new expressions will be “controller” and “processor”.

- “data processor”, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

2.4 The ICO does recognise that, in reality a processor can itself exercise some control over the manner of processing – e.g. over the technical aspects of how a particular service is delivered.

2.5 In the context of the HOB Programme:

- Chief Constables will be Joint Controllers for the fingerprint marks and DNA samples collected within their force.
- As the National Police Chief’s Council (NPCC) representative, the Chair of the Forensic Information System Databases (FINDS) is the controller in common.
- The Home Office will be the processor for information held on IDENT1 and NDNAD
- The Home Office is the controller (UK Visas & Immigration), and the processor (HOB) for information held on IABS.

Overarching HOB privacy considerations

2.6 The HOB programme recognises the importance of balancing public safety with individual privacy. In addition, it is essential that the public have confidence that personal information contained in biometric systems will be properly protected, and handled in accordance with the law.

2.7 The HOB Programme also recognises that there are significant ethical issues in the collection and use of biometric information. To make sure that the Programme undertakes the appropriate level of ethical scrutiny of the developing biometric technology, a HOB Ethics Working Group is in place to monitor the progress of the Programme and to review individual project PIAs.

2.8 All aspects of the HOB Programme require compliance with relevant law, including the Data Protection Act 1998, the Human Rights Act 1998, the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014, the EU General

Data Protection Regulation (GDPR), any further legal developments in this field, and, where necessary, the availability of appropriate data sharing arrangements[9].

2.9 The privacy impact of the retention and use of biometric information about individuals must also be considered alongside the operation and development of Home Office biometrics services; either as part of a criminal investigation or in an immigration context. The collection, storage and use of such information will only be legal and ethical if the interference with an individual's privacy is necessary, proportionate and in pursuit of a legitimate aim; and complies with legislation governing the use and retention of biometric data as well as data protection law.

Physical management of biometric data

2.10 The physical separation of the data that currently exists in Home Office biometric systems is as a result of the siloed evolution of these systems. This environment provides safeguards against inappropriate access to the data. However, the impact of holding data physically separate is that the Home Office has to support and maintain multiple systems, which is costly and complex, and introduces unnecessary delays and a greater likelihood of introducing data entry errors due to manual processes in operation.

2.11 The overall implementation of the strategic biometric services infrastructure has the potential to bring biometric data sets together. Going forward, data security will be based on logical separation rather than the current physical separation. Data will be held for different purposes, on a shared infrastructure, with business rules and security controls and the strategic governance defining which data collections can interact with one another to prohibit unauthorised access and usage, and so maintain the safeguards of personal data.

The HOB Information Security Management System (ISMS) document states that access control must be maintained for all HOB systems. Access Control for HOB systems is addressed by each of the individual subsystems and legacy systems, with authentication and authorisation distributed across the Biometric Services Platform

[9] Now the Data Protection Act 2018 has come into force, the HOB Programme PIA and existing project PIAs will be reviewed at the most appropriate time against the new data protection principles. Any new developments and projects will be assessed using the DPIA template.

(and described in the Programme Security Architecture). Defence in depth is used as a principle to enforce each security function.

The key components of the ISMS are as follows:

- **User authentication.** Users connecting by any means other than via the BSG shall be uniquely identified. User credentials must only be issued according to a formal registration process and users must possess appropriate security clearance before being issued with credentials.
- **System authentication** between HOB systems and between HOB and external systems.
- **Connection authorisation.** By preference all connections to the HOB BSP will be through the BSG as the secure gateway for access to HOB systems. Any new connection to the BSG will go through tight governance for approval.
- **User authorisation**. Users of the web portals and Bureau must be authorised to use the HOB BSP and for specific functions within it. This will be addressed by the individual system and the applicable Governance Board. Users will be afforded access on the basis of their role and their clearance.
- **Data Sharing Agreements.** The sharing biometric data will be strongly governed by Data Sharing Agreements approved by the controller with the data sharing partner supplying or receiving the data.
- **Supplier authorisation.** As a general security principle, a minimal number of support roles in any supplier should have access to the business data as part of their roles (i.e. biometrics and biographics).
- **Accountability.** Any HOB system must capture audit trails pertinent to its user and administrative activities.

2.12 The approach HOB takes to access controls, as outlined above, follows the “Defence in depth” principle that is used to enforce each security function and contributes to the protection of an individual’s privacy with the accumulation of data.

HOB decision to produce PIAs

2.13 In order to consider the full impacts of individual elements of the Programme and the cumulative impact of the changes, HOB has made a commitment to undertake a programme PIA in the Home Office Biometrics Business Case and the

Home Office Biometrics Strategy. This is also in accordance with Cabinet Office Best Practice for Major Government Programmes and is in line with ICO guidance.

2.14 Despite being a predominantly technology based programme, HOB is looking beyond the standard PIA assessment to identify any gaps in the hand-offs between the technology it is delivering, other IT Programmes and the operational staff who will use the technology (police forces, immigration enforcement, border force, etc). By looking at the Strategic Mobile area initially, the broader review will look at the hand off and crossover points in respect of:

- The biometric technology that is available to police forces to use in their operational work
- The touch points at which police forces collect and then use biometric information for operational purposes
- The operational guidance available to police forces that instructs them on the proper use of the biometric technology and information
- The legislative basis upon which police forces are able to collect and make use of biometric information.

Where the HOB project PIA does not cover subsequent operational use of the data, the Programme will work with subject experts (e.g. operational, legal, policy, technical) to identify resolutions and mitigations.

2.15 The HOB Programme PIA, will seek to:

- Identify and manage the risks that privacy issues represent to realising the intended benefits of HOB.
- Consider the risks of the aggregation of data, in particular, against the risk of potential injustice to individuals and groups of individuals.
- Generate information to aid decision making and support good governance and business practice around information processing.
- Identify Data Protection legislation to be considered during the build therefore ensuring compliance.
- Identify any necessary privacy features so these can be designed in at an early stage rather than be subject to costly retro-fitting at a later stage.

- Promote public confidence to maximise the information that people are prepared to disclose to the police and within immigration and nationality processes and reduce the risks of privacy related incidents that could undermine public confidence through injustice or potential harm.

2.16 It is acknowledged that the greatest benefit from a PIA is when it is embedded in, and used, as part of the project management tool set, used alongside programme requirements and allowed to develop to reflect changes. As such each project PIA within the HOB Programme will be developed during the project lifecycle process and then reviewed, following delivery, on an annual basis or when there is significant change to the technology if sooner.

Section 3: Methodology

3.1 Through answering the screening questions contained in the Information Commissioners Office PIA Code of Practice (2014) it can be identified whether a PIA is necessary.

3.2 The HOB screening questionnaire is included at Annex B and provides an overview of the data purpose, use and retention held on both IDENT1 and IABS.

3.3 The approach for the HOB Programme was to move to a disaggregated structure; to support this decision a series of PIA reflecting the strategic approach to building programme capacity are being produced. These PIAs will be appended to this Programme PIA which will consider the overarching impact of the programme.

3.4 The PIA Code of Practice suggests the following form and structure for a PIA:

- Describing the information flows – looking at what information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information.
- Identifying the privacy and related risks – this includes risks to individuals such as damage caused by inaccurate data or a security breach; it also includes distress from an unnecessary intrusion into an individual’s privacy. Risks to the organisation should also be considered such as loss of reputation or the financial consequences of a data breach. Consideration must also be given to legal compliance risks.
- Identifying and evaluating privacy solutions – consideration of how each privacy risk can be eliminated or reduced to an acceptable level, including evaluating the likely costs and benefits of possible options.

3.5 In addition, the following should be conducted:

- **Privacy law compliance check** - focuses on compliance with various “privacy” laws such as Human Rights Act, Protection of Freedoms Act 2012 (PoFA), as well as the Data Protection Act (DPA) 1998[10]. Examines compliance with statutory powers, duties and prohibitions in relation to use and disclosure of personal information.

[10] Replaced by the Data Protection Act 2018

- **Data protection compliance check** – a checklist for compliance with DPA. Usually completed when the project is more fully formed.

3.6 Recording the PIA outcomes – A PIA report should summarise the process and the steps taken to reduce the risks to privacy, recording the decisions taken to eliminate, mitigate or accept the identified risks. These decisions should be signed off at an appropriate level.

3.7 Review – This sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. It looks at new aspects of the project and assesses whether they should be subject to a PIA.

3.8 The HOB strategic project PIAs have all been subject to a consultation with a small number of interested parties during their development. This has ensured consideration has been given to privacy risks in all aspects of the technical developments.

3.9 In addition to the consultation, extensive internal analysis has been carried out, looking at relevant issues, together with additional issues arising from ethical implications of the aggregation of information and the potential for injustice. These continue to be explored and the outcomes used to inform the development of the Programme, particularly in relation to reducing risk by implementing measures to protect and enhance privacy.

3.10 In carrying out this work, it was the Programme's aim not just to make sure that it was meeting the minimum legal requirements but to minimise, as far as possible, given its objectives, the risk of impact on individuals' privacy. The Programme is following the concept of "privacy by design", incorporating privacy and security measures at the design stage of the project in line with current good practice.

3.11 The detailed user requirements that involve IT are fed into the business requirements supplied to the project architects, and subsequently the appointed supplier, to address the design, build and operation of the system. Those projects involving business process redesign will inform work to set policies and business rules for the data when it is to be located in the programme and for the future use of the systems.

3.12 As this work progresses, account will be taken of new legislation, official reports, reviews and recommendations as they become available. Where law enforcement parties are the controller and HOB is the processor steps will be made to ensure that identified areas of policy and guidance are reviewed and updated to ensure compliance.

3.13 The HOB programme objectives have been discussed with the Information Commissioner’s Office (ICO) and its views obtained; ongoing liaison with the ICO will inform the future development of the services in relation to privacy issues.

3.14 The HOB Programme is also undertaking an analysis of the touch points between the technology and front line operations to ensure there are no gaps in guidance, policy, powers, etc. This will involve wide range of internal and external stakeholders.

3.15 The Programme understands and supports the principles that are set out in the Data Protection Act 2018 which came into force in May, and the HOB Programme PIA and existing project PIAs (developed and approved under the DPA 1998) will be reviewed at the most appropriate time against these new data protection principles. Any new developments and projects will be assessed using the DPIA template.

3.16 Section 5 sets out the plans for formally reviewing, auditing and updating PIA assessments. This will include, as a minimum, the requirement to submit an updated PIA as part of the change control process. However, work will continue to ensure that privacy requirements are fully considered in the detailed design of the programme and the business processes around the data located on it.

Section 4: Findings on privacy risks and mitigations

4.1 The following table outlines the main privacy risks which have been identified as significant to the HOB Programme and requiring consideration as part of the PIA process

Risk	**Mitigation**	**Result** - is the risk eliminated, reduced or accepted?	**Evaluation** – is the final impact on individuals after implementing each mitigation a justified, compliant and proportionate response to the aims of the project?
The aggregation of personal data and whether this might pose a risk of injustice	The HOB programme is a technical programme and will develop solutions that work within the policy and legal frameworks set out, and the rules that apply, working with policy and legal teams to achieve this. Where data is held for different purposes on a shared infrastructure business rules and security controls will clearly define which data collections can interact with one and other to prohibit unauthorised access and usage. Access to the data by automation or manual processes will be enforced through 'role based access control' which restricts access to a	The risk is **accepted**	An evaluation of the risk will be completed every 6 months with an update included in the table

	process or piece of data, and makes sure that only authorised people can access the data, and only for the right process Compliance with privacy guidelines is important to the Programme, as is the consideration of potential impacts on individuals and groups, and the ethics of using biometric information. PIAs (and future DPIAs) will always be used as a mechanism to address such concerns. Where technology is used by front line staff, , HOB will work with policy and operational users to ensure that guidance reflects the capability that HOB is providing to the user		
The biometric information collected is seen as unfair or intrusive	The HOB Programme is committed to undertaking PIAs for all of its projects to identify potential impacts on individuals and groups. HOB will make sure that the technology implemented will address any recommendations highlighted through the PIA and that the solutions work within the policy and legal frameworks set out, and the rules that apply	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table

Biometric information is unnecessarily collected (and retained) without adequate justification	The PIA outlines the legal powers through which biometric data is collected, used and retained on HOB systems. Where the retention of biometric data is stated within legislation, the technology will be designed to meet the retention requirements, alongside the operational actions to delete records	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table
People are not given enough information or warning about the purposes of the collection of biometric information from them	It is a key principle that people understand why their biometric information is being collected and the ways the information will be used. The current immigration and law enforcement processes (e.g. application forms, guidance, etc) do state the reasons for biometrics being collected and organisations have Fair Processing Notices that state how an individual's data will be maintained. These are being updated to comply with new Data Protection legislation. Where technology is used by front line staff, HOB will work with policy and operational users to ensure that	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table

	guidance reflects the capability that HOB is providing to the user. Where the use, or re-use, of biometric data through the development of technological capabilities, may impact an individual, a PIA will consider these risks. The PIA will be considered through the appropriate governance to make sure that the risks are fully assessed and mitigated.		
Biometric information is used for purposes that are not what they were collected for	This is a very sensitive issue and is why the HOB Programme has undertaken PIAs for the projects to show that the biometric data is used for the purposes for which it is provided and within the policy and legal frameworks. HOB will continue to work with policy and legal teams to understand the policy and legal grounds on which the data is obtained and ensure rules are followed. Where there are changes in technology or legislation a PIA will be completed to assess impacts on privacy. Where data sharing arrangements are set up with other agencies, Government Departments and International	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table

	Governments, the appropriate Information Sharing Agreement (ISA) or Memorandum of Understanding (MOU) are produced		
Biometric information is retained longer than necessary	Where the retention of biometric data is stated within legislation, the technology will be designed to meet the retention requirements through automation, alongside the operational actions to delete records. There are circumstances where manual actions are required to assess the retention and deletion of records	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table
Information sharing arrangements with other agencies and organisations puts personal biometric information at risk	Where data sharing arrangements are set up with other agencies, Government Departments and International Governments, the appropriate Information Sharing Agreement (ISA) or Memorandum of Understanding (MOU) are produced	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table
Outsourcing to external suppliers does not adequately protect biometric	Privacy considerations are included in any tendering processes, negotiations and contracts for outsourced developments and handling of biometric	The risk is **eliminated**	An evaluation of the risk will be completed every 6 months with an update included in the table

information	information. Supplier contracts will be monitored to ensure that the privacy responsibilities are fully met. New data protection laws will strengthen the rules by which personal data is held and HOB is working with suppliers to be compliant with the new arrangements		
Extra expense is incurred because systems are not designed with privacy considerations	HOB is committed to "privacy by design" for all biometric developments and projects are supported by the development of privacy impact assessments at an early stage HOB is working to understand and act upon the impacts that the new EU Data Regulation and Directive will have on projects when implemented in May 2018	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table
Authorisation to access biometric information is not controlled and there is unauthorised access to the data	There is a clear security governance in place for central HOB technology Where necessary access to technology will be through Role Based Access Controls	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table

Loss of biometric information	HOB ensures that the biometric technology and service management has appropriate security environment for biometric information. As the new suppliers are brought on board this will continue to be a key feature of the contract arrangements Protocols are, and will continue to be, in place for the storage and handling of biometric information. Contingency plans are, and will continue to be, in place to address any security breaches. HOB is working to understand and act upon the impacts that the new EU Data Regulation and Directive will have on projects when implemented in May 2018	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table
Biometric information is incorrectly linked with a person which could lead to that person having an incorrect decision made against them	There are processes for handling false negatives and false positives when matching biometrics. However, the risk of error is very important. There will be ethical consideration of each project to identify any aspects of the technology (or process) that might impact on an	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table

	individual through their information being incorrectly linked to another. The risk assessment will identify any mitigating actions that a project might need to address. The technology is designed to enable records to be amended and/or deleted as appropriate where cases of incorrect information are identified.		
There is not a consistent, central Programme overview of personal information management or privacy risk	Privacy is a prime consideration for the HOB Programme and all HOB projects and a PIA is developed in all cases Governance is in place with HOB and the wider Home Office and operational businesses where privacy matters are considered	The risk is **eliminated**	An evaluation of the risk will be completed every 6 months with an update included in the table
A hack into the HOB system could impact on the protection of personal information. The potential damage of a hack is greater within the integrated system, rather than the current smaller constituent parts in the siloed system	HOB ensures that the biometric technology and service management has appropriate security environment for biometric information. As the new suppliers are brought on board this will continue to be a key feature of the contract arrangements. Through the security features of technology every effort is made to protect HOB systems from an intrusive	The risk is **reduced**	An evaluation of the risk will be completed every 6 months with an update included in the table

	attack on personal data from hackers		

Section 5: How the Programme will undertake an ongoing review, audit and updating of the Privacy Impact Assessment

5.1 The purpose of the "Review and audit phase" of a PIA is to check whether the actual impacts on privacy are those that were anticipated and that the actions that emerged from the PIA have been taken forward and are having the expected effects. Where either is not the case, it allows further action to be taken to assess the impacts and to take appropriate additional action as necessary.

5.2 Impact on privacy will be something that the HOB Programme will continue to consider at all stages as the programme progresses. It is anticipated that reviews will be conducted on an annual basis.

5.3 There will also be ongoing activities to:

- continue developing the organisational understanding of privacy and of the key privacy issues that arise
- reinforce recognition of privacy matters in project processes
- maintain an internal communications programme that keeps privacy in the minds of the Programme, operational staff, managers and senior managers
- maintain an external communications programme

Annexes

Annex A: Descriptions of the main biometric databases

Immigration and Asylum Biometrics System (IABS)

IABS is the biometric system used by immigration functions. IABS captures, stores, searches, matches and provides controlled access to 25m facial and fingerprint images. IABS was developed, supported and hosted under a seven year service contract with IBM which was signed in May 2009 (this system went live in February 2012) and planned to run until April 2016. This has been extended until April 2019.

The IABS system replaced an earlier system called IAFS, which has now been de-commissioned. Records and data from the IAFS system have been migrated onto the new IABS system.

Official – sensitive: start of section

The information on this page has been removed as it is restricted for internal Home Office use

Official – sensitive: end of section

IDENT1 (Law Enforcement and Security Biometrics System)

The IDENT1 Service provides the principle means of forensically verifying or resolving identities throughout policing, using fingerprints. It is used by fingerprint practitioners to verify the identity of up to a million people each year people each year taken into custody and arrested or detained, as well as to link some 80,000 scenes of crime marks each year to previously proven identities. Together with the Police National Computer (PNC) and the National DNA Database, it is a critical part of the police and criminal justice national infrastructure.

The police have the power to take fingerprints from Every person arrested in England, Scotland, Wales and Northern Ireland for a recordable offence and it is policy that this should always be done. The fingerprint data is aligned with the arrest event on PNC so that the arrest event details are unequivocally and unambiguously associated with the correct individual’s record on PNC.

IDENT1 provides much more than a singular database. The partitioning of different types of records into separate collections, together with carefully controlled workflow and access permissions which are set according to specific roles, ensure that the right information – and only the right information – is searchable in each particular circumstance. This is necessary to meet the legislation, codes of practice and privacy concerns associated with handling of Protected Personal Data as well as security and information assurance obligations.

IDENT1 is a distributed system that provides the services to maintain the national collection of tenprint records ("the Unified Collection") and the national collection of Unresolved Crime Scene Marks for fingerprint and palm-print searching and identification, as well as various specialist collections. The IDENT1 system consists of two national data centres, 53 force bureau systems, a few specialist bureaux and around 400 Livescan systems and connecting networks. IDENT1 has interfaces to PNC, SIS.II, local Custody systems, local forensic imaging systems, immigration, asylum and visa systems and others. IDENT1 is linked to the Police National Computer (PNC) Phoenix Criminal Justice Record Service to provide biometric assurance of criminal history records. The IDENT1 system is available 24 hours per day, 365 days per year except for short periods of planned and authorised down time for system maintenance or software releases.

IDENT1 is also used by the National Crime Agency, Counter Terrorist Command and the MOD.

The Forensic and Biometric Initial Capability (FABrIC) project delivered an interim continuity of the IDENT1 service contract that expired in March 2015. The FABrIC contract has been extended as part of the HOB programme until March 2019.

National DNA Database

The National DNA Database (NDNAD) is a national system which identifies links between DNA found at scenes of crime with DNA obtained from arrestees. 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. It is managed in house by the Forensic Information Databases (FIND) Service which ensures the integrity of the records on the NDNAD. The NDNAD is one of the largest DNA databases in the world, holding approximately 6.3m DNA profiles taken from arrestees and 487,000 DNA profiles obtained from scenes of crime samples. Conversion of a DNA sample into a DNA profile is carried out by outside laboratories***.***

Annex B: Privacy Impact Assessment Screening Questionnaire (published separately)

Annex C: Legislation references

Legislation	Link
Data Protection legislation	
Data Protection Act 1998[11]	http://www.legislation.gov.uk/ukpga/1998/29/contents
Freedom of Information Act 2000	http://www.legislation.gov.uk/ukpga/2000/36/contents
Law enforcement legislation (in England & Wales)	
Police and Criminal Evidence Act 1984	http://www.legislation.gov.uk/ukpga/1984/60/contents
Protection of Freedoms Act 2012	http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted
Anti-Social Behaviour, Crime and Policing Act 2014	http://www.legislation.gov.uk/ukpga/2014/12/contents/enacted
Criminal Procedure and Investigations Act 1996 & Codes of Practice	https://www.gov.uk/government/publications/criminal-procedure-and-investigations-act-code-of-practice
Crime and Security Act 2010	http://www.legislation.gov.uk/ukpga/2010/17/contents
Criminal Justice and Public Order Act 1994	http://www.legislation.gov.uk/ukpga/1994/33/contents
International Criminal Court Act 2001	http://www.legislation.gov.uk/ukpga/2001/17/pdfs/ukpga_20010017_en.pdf
Immigration legislation	
Immigration Act 1971	http://www.legislation.gov.uk/ukpga/1971/77/contents
Immigration and Asylum Act 1999	http://www.legislation.gov.uk/ukpga/1999/33/contents

[11] Now replaced by the Data Protection Act 2018

Asylum and Immigration (Treatment of Claimants, etc.) Act 2004	http://www.legislation.gov.uk/ukpga/2004/19/contents
Nationality, Immigration and Asylum Act 2002	http://www.legislation.gov.uk/ukpga/2002/41/contents
The Immigration (Provision of Physical Data Regulations) 2006	http://www.legislation.gov.uk/uksi/2006/1743/pdfs/uksi_20061743_en.pdf
UK Borders Act 2007	http://www.legislation.gov.uk/ukpga/2007/30/contents
The Immigration (Biometric Registration) Regulations 2008	http://www.legislation.gov.uk/ukdsi/2008/9780110818382/contents
The Immigration (Biometric Registration) (Civil Penalty Code of Practice) Order 2008	http://www.legislation.gov.uk/ukdsi/2008/9780110818320/contents
Immigration, Asylum and Nationality Act 2006	http://www.legislation.gov.uk/ukpga/2006/13/contents
Borders, Citizenship and Immigration Act 2009	http://www.legislation.gov.uk/ukpga/2009/11/contents
Immigration Act 2014	http://www.legislation.gov.uk/ukpga/2014/22/contents/enacted
EC Council Regulation 2725/2000: EU Eurodac Regulations	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33081
Council Regulation (EC) No 1030/2002: Uniform format for residence permits for non-EU country nationals	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Al33043

Annex D: HOB Project PIAs

HOB made a commitment (under the DPA 1998) to undertake a programme PIA, consisting of a suite of individual PIAs for each project as well as an overarching programme level PIA. Now that the Data Protection Act 2018 has come into force, the HOB Programme PIA and existing project PIAs will be reviewed on a rolling schedule. All PIAs for capabilities going live after the new Act came into force will be assessed using the new Data Protection Impact Assessment (DPIA) template, against the new data protection principles.

Project	PIA status
1. Strategic Mobile	Completed (under DPA 1998)
2. Biometric Services Gateway (BSG)	Completed (under DPA 1998). Version included but currently undergoing review
3. Strategic Matcher	Completed (under DPA 1998). Version included but currently undergoing review
4. Strategic DNA	Not yet ready for publication as under development
5. Prüm	Original version completed in 2015 (under DPA 1998) but not included as undergoing full refresh
6. Strategic Facial Matching for Law Enforcement	Not yet ready for publication as under initial development
7. Latent Mark searches of immigration data	Completed (under DPA 1998)
8. Strategic Central Bureau Project	Not yet ready for publication as under initial development
9. Bureau Tools	Not yet ready for publication as under initial development
10. Livescan Pilot	Initial completion under DPA 1998. Review underway against DPA 2018 prior to pilot go live

Annex E: Consultation

For this iteration of the HOB Programme PIA, and specific project PIAs, the following stakeholders have been consulted:

- HOB team members (including project leads, security architects, technical analysts and business analysts, Test Team)
- Policy specialists – Immigration and Law Enforcement
- Home Office Legal Advisors
- Operational teams (e.g. HMPO, Border Force)
- Information Commissioner’s Office
- Ethics Working Group

Annex F: Legislation summaries (published separately)

Annex G: Glossary

1:1	One to one
1:M / 1:N	One to many[12]
ACRO	ACPO Criminal Records Office
BRP	Biometric Residence Permit
BSG	Biometric Services Gateway
CID	Case Information Database
CTFS	Counter Terrorism Forensics Service
DBS	Disclosure and Barring Service
DNA	Deoxyribonucleic Acid
DVLA	Driver and Vehicle Licensing Agency
DWP	Department for Work and Pensions
EU	European Union
FCA	Financial Conduct Authority
FCO	Foreign and Commonwealth Office
FINDS	Forensic Information Databases Service
FR	Facial Recognition
FRS1	Facial Recognition Service 1 (HMPO Facial Watchlist)
FSP	Forensic Service Provider
HMG	Her Majesty’s Government
HMPO	Her Majesty’s Passport Office
HMRC	Her Majesty’s Revenue and Customs
HOB	Home Office Biometrics
IABS	Immigration and Asylum Biometric System (used as shorthand for UK’s immigration fingerprint database)
ICC	International Criminal Court
IFB	Immigration and Asylum Fingerprint Bureau
IDENT1	IDENT1 is an identity management system and scenes of crime forensic system; term used as shorthand for the UK’s criminal fingerprint database.
MoD	Ministry of Defence

[12] 1:M & 1:N – is used across different areas but always means more than 1:1 matching

NBTC	National Border Targeting Centre
NFO	National Fingerprint Office
NCA	National Crime Agency
NDNAD	National DNA Database
NDU	NDNAD Delivery Unit (Former name of FINDS-DNA Unit)
NPCC	National Police Chief’s Council
PACE Act	Police and Criminal Evidence Act
PIA	Privacy Impact Assessment
PNC	Police National Computer
PSNI	Police Service of Northern Ireland
SIA	Security Industry Agency
SFO	Serious Fraud Office
SMTP	Simple Mail Transfer Protocol
UKVI	United Kingdom Visas & Immigration