Home Office Biometric Programme - Privacy Impact Assessment - Strategic Mobile

This PIA was agreed on 17th November 2017

PIA Initial Screening Checklist

Programme/project/policy: Home Office Biometrics Strategic Mobile Project

The Strategic Mobile project within the Home Office Biometrics programme exists to support both the replacement of mobile biometric identity resolution capabilities in police forces and to deliver such a capability to Immigration Enforcement and other Home Office users. It is intended to supersede both the MobileID and RapID capabilities in use at present, providing the basis for a long-term, extensible, lower cost capability. It is envisaged that this capability will support a unified user experience, in turn driving greater operational effectiveness and enabling more accurate decisions to be reached based on more complete information being available.

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

Question	Yes	No	N/A
Will the policy involve the collection of new information about individuals?		X	
Will the project compel individuals to provide information about themselves?		X	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		X	
Are you using information about individuals for a purpose it is not currently used for, or in a		X	

way it is not currently used?			
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	X		
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	X		
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	X		
Will the project require you to contact individuals in ways which they may find intrusive?		X	

If it has been decided not to undertake a PIA please outline the reasons here:

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

Home Office Privacy Impact Assessment
Identify the need for a PIA: Explain what the project aims to achieve, what the benefits will be to the Home Office, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions). Remember a PIA is an evolving document, so there probably won't be definitive answers to all these questions. Rather, it will identify issues and risk that may need solutions.

The Home Office Biometrics (HOB) programme is seeking to replace existing biometric systems IDENT1, IABS[1] & NDNAD[2] used by the Police, Border Force, United Kingdom Visas and Immigration (UKVI) and HMPO. It will implement a single biometrics service that will deliver continuity of business services once the current contractual arrangements end, delivered by sub-programmes over a period of 3-4 years.
As part of the above the HOB strategic disaggregation and transformation programme (a collection of strategic projects) will transform the existing separately siloed IT capabilities via a platform using role based access controls creating a single converged, but disaggregated, strategic capability. Respecting individual rights, freedoms and civil liberties is central to this work. Strategic Mobile is one of the projects being delivered within this programme.

The current mobile biometric solutions are nearing end of life, are now costly and of limited utility to its users. The Home Office Biometrics (HOB) programme will support both the replacement of mobile biometric identity resolution capabilities in police forces and to deliver such a capability to Immigration Enforcement and Border Force.

It is expected that the Strategic Mobile capability will follow a phased approach:
1. Support police forces who currently use MobileID, and their mobile solution providers;
This approach will introduce biometric-assured identity resolution to the existing Police National Computer (PNC) and local force mobile criminal history search capabilities in forces
2. Implement an equivalent capability for Home Office users (including Immigration Enforcement and Border Force)
3. Support the evolution of an enhanced search capability. (Combined data source as a result of converging the database access.)
4. Support the mobile biometric search capability to other users groups.
5. Enable capability for future enhancements.

[1] 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

[2] NDNAD – the National DNA Database holds electronic DNA profiles and identifies links between DNA found at scenes of crime with DNA obtained from arrestees (and on occasion other individuals such as vulnerable persons and missing persons)

Describe the information flows: You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

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

Consultation requirements: Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. You can use consultation at any stage of the PIA process.

A PIA was previously completed for mobile capability however in view of the current changes being undertaken under the Home Office Biometric Programme this PIA has been completed afresh. The Information Commissioner's Office (ICO) and the Home Office Biometrics Ethics Group (HOB EG) will be consulted during the development of this PIA.

The updated PIA will be submitted to the Strategic Mobile Project Board, the HOB programme Board, The Home Office Legal Advisers (HOLA) and the Information Commissioners Office (ICO). Any privacy risks identified from this PIA will be included in the projects risk register and addressed and mitigated in line with project methodology.

The views of the business areas will be represented through both the Strategic Mobile project Board and the HOB programme board. As part of the overall assessment of the HOB programme the Cabinet Office will be engaged and informed of this project's aims.

Biometric data captured and transmitted by mobile consumers is minimal and not stored. There will be a record of the interaction with the individual but no other records will be held. Pocket book notes of the Police or Immigration Officer* are captured including location, date, time, officer, perceived ethnicity and given name. * This data capture is outside the scope of the mobile project

The security of the mobile technology will be assured via an appropriately evidenced set of mandated security (privacy) controls that are defined within the Biometric Services Gateway (BSG) Code of Connection – many of these controls include strong cryptographic mechanisms such as transmission encryption and signing.

The security of the mobile technology biometric solutions will be assessed through the agreed HOB security assurance process. Mobile solutions are not granted access to HOB biometric collections unless the mandated security controls have been satisfied. This requirement is subject to annual assessment that triggers the re-issue of digital certificates to the consuming organisation. Should a consuming organisation overlook its annual assessment then its digital certificate will expire resulting in self-imposed disconnection.

Data Protection Act Principle 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: **a) at least one of the conditions in Schedule 2 is met, and** **b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**	
1.1 Why is the personal data being collected used, disseminated, or maintained?	The Strategic Mobile Project does not collect, disseminate or maintain information. The Strategic Mobile project, will process fingerprints for identification purposes, checking identity against records held on IABS (Immigration fingerprint database) and IDENT1 (The UK fingerprint database for policing). The project provides technology to support the control of immigration and the prevention, detection, and investigation of crime.
1.2 Where is the information collected from, how, and by whom?	The Strategic Mobile Project does not collect or store information, the information is checked against existing datasets held in IABS and IDENT1. Information is discarded once the check has been completed.
1.3 If collected by an organisation on behalf of the Home Office, what	The project is only responsible for enabling checks and verification of fingerprints held on the existing IDENT1 and IABS systems.

is the relationship and authority/control the Home Office has over the organisation? Who is the Data Controller and Data Processor? Is a formal agreement in place to regulate this relationship?	Collected by police and Immigration using powers set out in the Acts mentioned 1.8 This includes custody suites, Forensic and Immigration Bureaux, Scenes of Crime, UK borders, Visa enrolment centres, and on mobile devices by enforcement officers within in the UK and British Forces overseas. Data controller/ Processor: 1) Fingerprints and finger marks taken in relation to the investigation of crime • Analysis of fingerprints and finger marks is done within each police force. (NB as the mobile check does not search against finger marks they are out of scope for this PIA) • Chief Constables are all data controllers for fingerprints and finger marks collected within their force. • The Chair of the FIND Strategy Board is the data controller in common. The HO is the data processor. 2) Fingerprints collected for the immigration purposes • The HO is data controller
1.4 How will you tell individuals about the use of their personal data? Do you need to amend your privacy notices? Is this covered by the Home Office Personal Information Charter?	No, Out of scope as the project provides a technical service and does not interface with individuals. However in line with existing practice the individual will be advised that fingerprints are being taken for identification purposes. Yes - for Home Office purposes information is on line: https://www.gov.uk/government/organisations/home-office/about/personal-information-charter

1.5 Have you established which conditions for processing apply?	No The Strategic mobile project does not process the data it merely accesses existing datasets to check and verify identity.
1.6 If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	No The Strategic mobile project will enable the capability to check and verify fingerprints held on IABS and IDENT1.
1.7 What information is collected, used, disseminated, or maintained in the system?	None, No fingerprints or other personal data will be retained beyond the point at which they are required for search and verification relating to confirming identification.
1.8 Is there a specific legal power that enables the gathering and use of the information? Does the power mandate the collection of the data or merely permit it?	Yes With respect to Police use of MobileID - The power under section 61(6A) of PACE described in paragraph 4.3(e) allows fingerprints of a suspect who has not been arrested to be taken in connection with any offence (whether recordable or not) using a mobile device and then checked on the street against the database containing the national fingerprint collection. Fingerprints taken under this power cannot be retained after they have been checked. Section 63A (1A) PACE sets out how fingerprints can be searched against other databases. Subsection d) is relevant as it reads “a public authority (…) with functions in any part of the British Islands which consists of or include the investigation of crimes or the charging of offenders. The Secretary of State for the Home Dept is a public authority and, in relation to immigration crimes, she has functions relating to the investigation of crime. For Immigration purposes powers set out in the primary and secondary legislation: Immigration Act 1999 specifically section 20 & 21

	Nationality Immigration and Asylum Act 2002 UK Borders Act 2007 The Immigration Act 2014 (Aligned immigration powers around retention and use of biometrics). For the purposes of this PIA it should be noted that the mobile project's responsibility ends at the point of data transfer. The policy and guidance will be reviewed to consider any further impact outside of the current scope of this PIA as part of the hand off exercise with the business.
1.9 Is there a specific business purpose that requires the use of this information?	Yes There is a business requirement for mobile identification functionality. The Strategic Mobile Project will make cross checking against immigration and criminal biometric data bases easier and more efficient. It will enhance the ability to deploy the capability through mobile technology at the border and as part of immigration enforcement operations, in the prevention and detection of crime and for public safety activity.
1.10 Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?	Biometric data captured and transmitted by mobile consumers is minimal and not stored. The security of the mobile technology will be will be assured via an appropriately evidenced set of mandated security (privacy) controls that are defined within the BSG Code of Connection – many of these controls include strong cryptographic mechanisms such as transmission encryption and signing. The security of the mobile technology biometric solutions will be assessed through the agreed HOB security assurance process. Mobile solutions are not granted access to HOB biometric collections unless the mandated security controls have been satisfied. This requirement is subject to annual assessment that triggers the re-issue of digital certificates to the consuming organisation. Should a consuming organisation overlook its annual

	assessment then its digital certificate will expire resulting in self-imposed disconnection. There will be a record of the interaction with the individual but no other records will be held. Pocket book notes, of the Police or Immigration Officer* are captured including location, date, time, officer, perceived ethnicity and given name. * This data capture is outside the scope of the mobile project.
1.11 Human Rights Act: Will your actions interfere with the right to privacy under Article 8? Have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?	Yes The aim of the project, which updates an existing capability, is to support the strategic aim of the prevention and detection of crime and to detect immigration offenders. Biometric identification using the mobile capability may be used when officers have been unable to establish identity based on biographical methods. In these circumstances it is a proportionate response to the problem of how to detect those who have committed a crime or immigration offences and how to confirm their identity.
Principle 2: **Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**	
2.2 What are the main uses of the information? Does your project plan cover all of the purposes for processing personal data?	Yes To validate identification
2.3 Have you identified potential new purposes as the scope of the project expands?	The project will make the existing capability quicker and more efficient**.**
2.4 Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?	Not applicable – the project does not collect information. In the process of a search the officer would receive a “yes” “no” answer in terms of a match providing a biometric reference which does not in itself identify an individual.
Principle 3:	

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
3.1 Is the quality of the information good enough for the purposes it is used?	Yes but it is not in the project scope to define what is collected and quality checks are done within the user Bureau (outside of the project scope).
3.2 Which personal data could you not use, without compromising the needs of the project?	None
Principle 4: **Personal data shall be accurate and, where necessary, kept up to date.**	
4.1 If you are procuring new software does it allow you to amend data when necessary?	No. The new software will just provide mobile access to existing data no amendments will be made to the existing data.
4.2 How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Not applicable
Principle 5 **Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.**	
5.1 What retention periods are suitable for the personal data you will be processing?	Not applicable Police use of MobileID - Fingerprints taken are not retained after they have been checked. Immigration use of RapID – Enquiry fingerprints are not retained after they have been checked.
5.2 Are you procuring software that will allow you to delete information in line with your retention periods?	No This project only enhances the capability to access data held and does not store data. The data collected is discarded after check has been completed.
5.3 Is the information deleted in a	Not applicable

secure manner which is compliant with HMG policies once the retention period is over? If so, how?	
5.4 What are the risks associated with how long data is retained and how they might be mitigated?	As above. The data is discarded after check has been completed
Principle 6 **Personal data shall be processed in accordance with the rights of data subjects under this Act.**	
6.1 Will the systems you are putting in place allow you to respond to subject access requests more easily?	No
Principle 7 **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**	
7.1 Who will have access to the system? Please provide role and responsibilities.	Access via mobile devices will only be granted to appropriate Law and Immigration enforcement officers. During a mobile search the officer will receive what is in effect a match, no-match response through their mobile devices this is minimal information but could lead to further investigation as per 2.4 above. Access control is protected as per 1.10 above. At this point there is not an expectation to allow an app accessed via personal devices. However this will be technically feasible but the app would still be securely controlled and the expectation would be that suitable, acceptable security protocols and software will need to be present for the app to be downloaded from a secure store.
7.2 What level of security clearance is required to gain access to the system?	As above all users will all be non police personnel vetting (NPPV) or security cleared (SC) at a minimum – in order to be given a device in the field.
7.3 Does the system use 'roles' to assign privileges to users of the system?	The system and the devices will have role based access security protocols.

7.4 How is access granted to the system?	Separate procedural security controls for Level 2 support and Level 3 support govern how access is provisioned within Lightweight Directory Access Protocols (LDAP) for each respective support team.
7.5 How are the actual assignments of roles and rules verified?	A procedural control (Joiners, Movers & Leavers process) provides a level of governance, whereby user access privileges are reviewed against user role to ensure principle of least privilege is maintained
7.6 How is this data logged and how is this reported to prevent misuse of data?	Security Information Event Management (SIEM) system provides a protective monitoring capability where transactions are logged and reports generated for review by Operational Security and others who have a need to know
7.7 What training is provided to cover appropriate use and basic security to users? How is the training refreshed? Is the training tiered?	Support personnel have undertaken security briefings that include basic cyber hygiene; this is in addition to Home Office standard security training predicated for POISE access. Additionally HOB Development Environment mandates reading and signing of Security Operating Procedures (SyOPs) that clearly articulates expected security behaviours and applicable security policies. Police users are subject to the IS awareness regime, acceptable usage policies and access controls of their individual forces.
7.8 Has or is the system going to be formally accredited using HMG standards to process and store the information, if so who is the accreditation authority (person/organisation)?	The mobile project will be subject accreditation by the National Policing Accreditor.
7.9 Given access and security controls, what privacy risks were identified and how might they be mitigated?	Separate procedural security controls for Level 2 support and Level 3 support govern how access is provisioned within LDAP for each respective support team. The mobile devices are under the control of a Mobile Device Management (MDM) solution from the point of provisioning (ensuring that the device is placed into a ‘known good’ state) and the MDM can remotely administer, configure, and audit mobile devices. The MDM must also have the ability to remote wipe mobile devices if reported lost, compromised or stolen.
Principle 8	

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	
8.1 Will the project require you to transfer data outside of the EEA?	No
8.2 If you will be making transfers, how will you ensure that the data is adequately protected?	Not applicable
9. Internal sharing within the Home Office	
9.1 With which parts of the Home Office is the information shared, what information is shared and for what purpose?	Not applicable
9.2 How is the information processed or disclosed?	Not applicable
9.3 What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?	Not applicable
10. External sharing and disclosure (If you have already completed a HO Data sharing toolkit then please attach and leave these questions blank).	
10.1 With which external organisation(s) is the information shared, what information is shared, and for what purpose? Has the Home Office specifically asked suppliers to undertake PIAs?	Not applicable
10.2 Is the sharing of personal information outside the Home Office compatible with the original	Not applicable The project does not store data

collection? If so, is it addressed in a data-sharing agreement? If so, please describe.	
10.3 How is personal information shared outside the Home Office and what security measures, compliance and governance issued safeguard its transmission?	Not applicable
10.4 Is a MoU in place for the Home Office to verify that an external organisation has adequate security controls in place to safeguard information?	Not applicable
10.5 Given the external sharing, what are the privacy risks and how might they be mitigated?	Not applicable
11. Notice	
11.1 Do individuals have an opportunity and/or right to decline to decline to disclose or share information?	Not applicable
11.2 Do individuals have an opportunity to consent to particular uses of the information, and how?	Not applicable
11.3 How could risks associated with individuals being unaware of the collection be mitigated?	Not applicable
12. Access, Redress and Correction.	
12.1 How are individuals notified of the procedures for correcting their	Not applicable

information?	
12.2 If no formal redress is provided, what alternatives are available to the individual?	Not applicable
12.3 What are the privacy risks associated with redress and how might they be mitigated?	Not applicable
Overview: What changes have been made or recommended as a result of the PIA process? At which key milestones in the project's lifecycle will the PIA be revisited? The projects risk register is held on the EPM Clarity tool and is available on request to the project team. The project delivery date for the Police - March 2018 Immigration and Enforcement is estimated to be approximately 6 months later The PIA will be revisited at key project milestones and as a minimum At 1. Procurement stage 2. pre Go-live 3. Post Implementation Review	

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
