Home Office Biometrics Programme - Privacy Impact Assessment - Strategic Matcher (Fingerprint) Phase 1a

This PIA was agreed on 1st August 2017

PIA Initial Screening Checklist
Programme/project/~~policy~~: The Home Office Biometrics (HOB) Strategic Matcher (Fingerprint) project will deliver a Biometric Matcher Platform and associated Service (BMPS) that ensures continuity of existing service and supports cost efficiencies through disaggregation and by using a common capability to replace the two separate matching capabilities in the legacy IDENT1 (law enforcement) and IABS (immigration) systems. The BMPS is a key subsystem providing biometric matching services to the rest of the HOB Services. The BMPS comprises: • Matcher Service Platform (MSP) and associated Services – a combination of a technology platform and the Services required to support and operate the biometric matching functions. The technology platform or MSP is further broken down into: - a Matcher Service Bus (MSB) where biometric transaction processing logic, workflow rules, associated biometric component, integration of MESs and a service interface used by external subsystems. - the infrastructure to host and provide the computing capacity for the MSB and MESs operations. • Matcher Engine Software (MES) – a combination of algorithm software and associated software that provide the specialised capability to match a biometric image to a known identity held as an encoded image. The BMPS Project will deliver capability in phases ("**Phases**"): • **Phase 1a** - There are two key deliverables for Phase 1a: - the delivery of a new MSP and Fingerprint MES that together form a BMPS with the capability to replace all of the existing IDENT1 IDENT 1 Centralised fingerprint matching capability; and - the migration of law enforcement IDENT 1 Centralised matching workloads from IDENT1 to the BMPS; • **Phase 1b** - There are two key deliverables for Phase 1b: - scaling and enhancement of the BMPS created in Phase 1a to provide the biometric matching capability to replace

all of the existing IABS fingerprint matching capability; and

- migration of the immigration fingerprint matching workloads from IABS to the BMPS.

The Strategic Matcher (Fingerprint) Project (Phase 1a) will deliver the Biometric Matcher Platform and associated Services. This comprises technology to support the biometric search, identification, and verification services currently provided by the matching capability in IDENT1[1].

Fingerprint data is collected from individuals (in custody suites and at crime scenes) and used to verify the identity of persons who are suspected of having committed crimes.

The Matcher Service will receive a request from IDENT1 to match print sets (tenprints, palms, or latents against a gallery of templated images) and the results will go back to IDENT 1.

This PIA covers Phase 1a of the Strategic Matcher project as described above. Phase 1b will be covered under a separate PIA. The need for separation/convergence of business data is being discussed and addressed in preparation for Phase 1b

Data Controller/Data Processor.

The Home Office is Data Processor for information held on IDENT1

Chief Constables are all data controllers for the fingerprint marks collected within their force. The Chair of the Forensic Information System Databases (FINDS) is the data controller in common.

Individual(s) completing PIA screening:

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

[1] IDENT1 is an identity management system and scenes of crime forensic system; term used as shorthand for the UK's criminal fingerprint database.

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 way it is not currently used?		x	
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: N/A			

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 IDENT[2], IABS[3] & NDNAD[4] used by the Police, Border Force, United Kingdom Visa 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. The Strategic Matcher is one of these projects and a key enabler, without which the wider programme will not be able to deliver. **The Strategic Matcher Supports the core Home Office Biometrics (HOB) objectives:** **1.** Ensure continuity of the biometrics capability **2.** Reduce IT costs (for a like-for-like service) **3.** Enhance capability **The Strategic Matcher (Fingerprint) Project** will deliver the Biometric Matcher Platform and associated Services (BMPS). This comprises technology to support the biometric search, identification, and verification services currently provided by the matching capability in IDENT1 and IABS systems.

[2] IDENT1 is an identity management and scenes of crime forensic system, term used as shorthand for the UK's criminal fingerprint database.

[3] IABS – provides biometric enrolment, identification, and 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

[4] NDNA – 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)

The BMPS is split into three main components:

- **Matcher Service Platform** - a combination of a technology platform and the Services required to support and operate the biometric matching functions.
- **Matching Service Bus** – containing the biometric transaction processing logic and rules (e.g. determination of which matching engines to search and co-ordination of responses), and presenting algorithm-agnostic services to the HOB IDENT 1 Central Service.
- **Matching Engine Software** – a combination of algorithms and associated components deployed as "Matching Engines" e.g. per modality, collection and matcher operation type. This will also include associated elements, such as biometric quality assessment and fingerprint segmentation algorithms, etc.

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.

The IDENT1 Service provides the principal means of forensically verifying or resolving identities throughout policing, using fingerprints. It is used by fingerprint practitioners to verify the identity of some 1,500,000 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.

Every person arrested in England, Scotland, Wales and Northern Ireland for a recordable offence has their fingerprints taken. This fingerprint data is aligned with the arrest event on PNC so that the arrest event details are associated with the correct individuals' 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 particular circumstances. 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 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 existing IDENT1 workflow processing will be unchanged in the immediate term, other than to re-point it at the new matching capability. A temporary adapter will be required to support this transient state i.e. to make it appear to legacy IDENT1 that it is still talking to its original matchers. Longer term convergence of IDENT1 Central and IABS Central is planned, but not addressed as part of the Matcher project nor this PIA.

The Strategic Matcher Project (Phase 1a) will deliver the Biometric Matcher Service. This comprises technology to support the biometric search, identification, and verification services currently provided by the matching capability in IDENT1. The Service has three main components:

- Strategic Matching Bus – containing the biometric transaction processing logic and rules (e.g. determination of which engines to search and co-ordination of the responses), and presenting algorithm-agnostic services to the HOB IDENT 1 Central Service.
- Matcher Engine Deployments – a flexible platform designed collaboratively to support deployment of Matching Engine Software.
- Biometric Matching Engine Software – a combination of algorithms and components deployed as "Matching Engines" e.g. per modality, collection and matcher operation type. Also elements, such as biometric quality assessment and fingerprint segmentation.

All fingerprint images (approx 10 million) will require re-encoding using the new algorithm. The fingerprint image (a 'temporary image') is received by the system for templating. The system will securely delete the 'temporary image' after templating (see 5.4). The image itself is not retained within the Matcher. Templates are the only Biometric Data that will be persisted, these are described in 5.4.

Business Data will be retained in line with existing data retention periods. There is expected to be an increase in the number of suspects identified, as a result of the enhanced matching capability, leading to more successful convictions. Improved accuracy will not just impact adversely on those identified, but also positively on those eliminated (from the criminal investigation). See **Annex A** for Diagrams.

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.

The HOB PIA has been seen and commented on by the Information Commissioners' Office and this PIA will form part of the overarching HOB PIA and submitted with the HOB PIA.

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

We continue to consul stakeholders through the Strategic Matcher Project Board, and groups, including the IDENT 1 Reps Meeting (IRM), and ongoing engagement with users (such a collaborative events); and the HOB Ethics Group working group. This includes the consideration of privacy issues, in defining non-functional requirements including information security.

Key stakeholders (users) for the Strategic Matcher project include:

- All 43 geographic police forces in England & Wales
- Police Service (PSNI) and Forensic Service of Northern Ireland (FSNI)
- Police Scotland and Scottish Police Authority (SPA)
- National Crime Agency (NCA)

• Forensic Service Providers (FSPs) • Fingerprint Bureaus of England and Wales, Scotland, and Northern Ireland • National Fingerprint Office (NFO) • OSCT/CT • UKVI • HMPO • Border Force • MOD	
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?	Fingerprint data is collected from individuals (in custody suites and at crime scenes) and used to verify the identity of persons who are suspected of having committed crimes. Section 63 of the Police and Criminal Evidence Act 1984 allows DNA and fingerprints legitimately retained in England and Wales to be used to prevent and detect crime outside England and Wales. Similar rules apply in Scotland and Northern Ireland under different legislation. As does legislation in the Crown Dependencies. See 1.4 below. The Police and Criminal Evidence Act and its Codes of Practice mandate the taking of DNA and fingerprints from arrested people and the Protection of Freedoms Act mandates the retention of such data if a person has been convicted of a recordable offence. The matcher service will receive a request from IDENT1 to match print sets (tenprints, palms, or latents against a gallery of templated images) and the results will go back to IDENT 1. As part of the implementation of the new matcher service, copies of ALL collections (Tenprints, palms, and latents) will be initially loaded into matcher to create algorithm specific segregated template galleries. After templating the images will be deleted. Images sent to matcher post go live will be turned into templates and ran through the matching algorithm. The temporary image will then be “deleted” (not persisted). See 5.4 below.
1.2 Where is the information collected from, how, and by whom?	Collected by Police Forces from individuals as custody samples and through crime scene investigation. Biographic data related to these profiles is supplied through Police National Computer (PNC). No additional personal data will be collected as a result of the new Matcher service.

1.3 If collected by an organisation on behalf of the Home Office, what 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?	Data Controller - For custody, and scene of crime images, collected under police powers regional Chief Constables are the data controllers for the data collected within their force. Data Processor - As the ministerial department responsible for policing the Home Office is data processor for custody images held on IDENT1 and will remain so.
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?	Suspects who are fingerprinted by the police in custody suites etc are informed how their data is used under existing procedures. The fingerprint (and palm) images are held on the IDENT1 system. The new matcher service does not change how data is collected or used by the police. Fingerprints (and DNA reference profiles) are taken from individuals following their arrest for a recordable offence using powers set out in the Police and Criminal Evidence Act 1984. Section 63 of the same Act allows DNA and fingerprints legitimately retained in the England and Wales to be used to prevent and detect crime outside England and Wales. Similar rules apply in Scotland (Criminal Procedure [Scotland] Act 1995) and Northern Ireland (Proceeds of Crime Order 2015). There is thus no change to the possible uses of DNA and fingerprints. The Privacy notice in England and Wales includes reference to possible use outside England and Wales. Crown Dependencies: Legislation re Fingerprints:- • Isle of Man - Police Powers and Procedures Act 1998 • Bailiwick of Jersey - Police Procedures and Criminal Evidence (Codes of Practice) (Jersey) Order 2004 • Bailiwick of Guernsey (Guernsey, Alderney and Sark) - The Police Powers and Criminal Evidence (Bailiwick of Guernsey) Law, 2003.
1.5 Have you established which conditions for processing apply?	Fingerprints are collected from individuals by Police Forces as custody samples, and through crime scene investigations. Biographical data related to these profiles is supplied through the Police National Computer (PNC). The fingerprint images and marks are searched against templated galleries to try and identify individuals suspected of committing criminal offences; and to eliminate others from the investigation. New fingerprint images will be templated to add them to the gallery and the image then deleted from the matching system.

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?	The process for enrolling fingerprints, and related biographical data, for policing does not rely on consent.
1.7 What information is collected, used, disseminated, or maintained in the system?	The fingerprint is received by the system for templating. The image itself is not retained within the matcher. The system deletes the image as soon as templating is complete.
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?	Section 63 of the Police and Criminal Evidence Act 1984 allows DNA and fingerprints legitimately retained in the England and Wales to be used to prevent and detect crime outside England and Wales. Similar rules apply in Scotland and Northern Ireland under different legislation. As does legislation in the Crown Dependencies. See 1.4 above. The Police and Criminal Evidence Act and its Codes of Practice mandate the taking of DNA and fingerprints from arrested people and the Protection of Freedoms Act mandates the retention of such data if a person has been convicted of a recordable offence.
1.9 Is there a specific business purpose that requires the use of this information?	Yes. This information is required to perform biometric identification and verification of individuals.
1.10 Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?	Privacy risks are deemed to be reduced through the nature of the data that is retained on Matcher. In principle, raw biometric images are not persisted on Matcher. All identity information (biometric and biographic) is mastered in IDENT1. Raw biometrics are initially sent to the Matcher from IDENT1 in order for the MES to carry out the initial encoding. These are not retained after the template is generated. Images are encoded into templates by the matching algorithm (provided by the MES) in a one-way function that redacts the image into the key machine-recognisable points used for matching. This is non-reversible and cannot be then used to reverse engineer a human-recognisable image. Individuals therefore cannot be identified by the templated data. Access to a secondary dataset (e.g. on IDENT1 or obtained from another source) would be required in order to resolve the identity from the template.
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	Not directly as replacing the algorithm (matcher) for IDENT 1 won't change how suspects are identified. The aim of the project is to provide improved matching capability enabling the identification of suspects, victims and missing persons. The sharing of information by the police is a proportionate response to the problem of how to detect who has committed crimes and

the project? Are your actions a proportionate response to the social need?	how to confirm the identity of arrested individuals.
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.**	
2.1 What are the main uses of the information? Does your project plan cover all of the purposes for processing personal data?	The fingerprint matching results are used to identify individuals who are suspected of having committed crimes; and to eliminate others from the investigation. The information required, and the request for the matching service is sent to the HOB matching service from IDENT1 system. The matching results may go to the police fingerprint bureau for manual verification by fingerprint experts (depending on thresholds etc.); and could be used for evidential purposes (i.e. in court). Algorithm thresholds will be decided at the Forensic Information Databases (FIND) Strategy Board. Those results automatically verified by the matching system will go back to the IDENT1 system directly. Those requiring manual verification will go to the bureau via the IDENT1 system. Information gathered, but not required for this purpose, will not be transmitted to the matching service as part of the service request.
2.2 Have you identified potential new purposes as the scope of the project expands?	The project will deliver in a number of phases, which have been identified as part of the Home Office Biometrics Strategy. If and when potential new purposes are identified as part of project expansion, for example facial images for law enforcement, then these will be assessed appropriately for privacy impact.
2.3 Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?	As stated at 1.10, privacy risks are deemed to be reduced. Individuals cannot be identified by the templated data whether held, or transitioning through the matcher system. Templates are stored with a unique reference number that can then be used to link back to biographic information held outside the confines of the system. Hardware and software associated with the Strategic Matcher is held only within appropriately accredited environments. There is an Identity Level Record in IDENT 1 Central. It would be necessary to recover the

	'Identity Level Record' and biographics (if available) from IDENT 1 Central and its mapping to Matcher Record References plus the templates from Matcher to derive the identity from a template. Therefore Matcher presents a lower risk than Central data, because once IDENT 1 Central has been breached there would be no further benefit in breaching a second system and to reverse engineer – the information has already been obtained.
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?	The quality of fingerprints is good enough for tenprints, but not for latents marks, as these vary in quality. The new matching algorithm (s) should help improve latent matching results – through enhanced capability.
3.2 Which personal data could you not use, without compromising the needs of the project?	The matching set up within IDENT1 is segmented to allow tenprint, latent, palm, hypothenar searching (See **Annex B**). These searches are against a gallery of prints/marks as follows:- • Searching of a ten print set against a gallery of other ten print sets. • Searching of a ten print set against a gallery of Unsolved fingerprint Latent marks. • Searching of a fingerprint latent mark against a gallery of ten print sets. • Searching of a Latent Palm mark against a gallery of palm prints. **The matcher does not use any personally <u>identifiable</u> biographical data (name and date of birth) as this could potentially identify the individual (data subject).** However, non-biometric, i.e. biographic/demographic, data will be used to provide biometric search binning or post search result filtering if required to do so by the request from the IDENT 1 Central Service. Non-biometric data that is provided as part of enrolments will be stored alongside or within the biometric engine(s) as appropriate, dependant on the functionality of the biometric engine to support this capability directly or not. The following fields could be used for this capability: - subject year of birth - subject gender - subject nationality - enrolment date

	- location code of original enrolment - enrolment case type - collection code **The above fields would not enable an individual (data subject) to be identified.** Non-biometric data will be managed in a similar manner to biometric data, providing facilities to support querying, addition, amendment, and deletion from a suitable request. No identity resolution could be made between data in the matcher (biometric data and associated metadata) and this biographical data without access to a separate platform to interpret the data (e.g. IDENT1).
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 only data is the fingerprint images (tenprints and palms) which are templated, and the unique identifier associated with that image). There will be a quality check and potentially capability to enhance the resolution of the image. All fingerprint images (approx 10 million) will require re-encoding using the new algorithm. HOB has a number of measures to protect the system from data quality issues that may occur following bulk import of biometric images:- 1) There is a MUST requirement on the Matcher Service Supplier to audit and report on the import of biometric data; and 2) We will prove the success rate and quality of bulk imported records including bulk encoding of images prior to live service in: a. Biometric Accuracy Testing (BAT) as part of the Matcher Procurement evaluation to select suppliers, b. Further BAT of the selected Matcher Service Supplier and Matcher Engine Software Supplier(s); and c. Data Migration Testing.
4.2 How are you ensuring that personal data obtained from individuals or other organisations is accurate?	The Matcher does not obtain its own data and IDENT1 has it own rules to ensure that data is accurate; Matcher will not change these rules.
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?	Fingerprint images and marks are only retained during templating and are then deleted. This is a requirement and how it is achieved will be agreed with the successful suppliers, and assured by HO security. Retention of the template will be subject to the same retention rules as govern fingerprints.
5.2 Are you procuring software that will allow you to delete information in line with your retention periods?	Yes this is included in the Strategic Matcher Non-Functional Requirements (NFRs)
5.3 Is the information deleted in a secure manner which is compliant with HMG policies once the retention period is over? If so, how?	Yes. The NFRs states that data must be deleted in accordance with the specified retention policy. The solution must perform deletion according to CESG Information Assurance Standard No5 – Secure Sanitisation, or in a manner agreed with the Authority. See also below:- Deletion of Records:- • Weeding of images for England and Wales arrestees is controlled by PNC, in line with The Protection of Freedom's Act 2012 (PoFA) legislation which amended the Police and Criminal Evidence Act (PACE), established a new regime to govern the retention and use of DNA samples and DNA profiles taken by the police in England & Wales. PNC makes the calculation to determine which records need to be removed and issues weed requests to IDENT1. This is an automatic process and occurs daily. As the images are removed from the database then relevant encodings are also removed from matcher engines. There are reconciliation scripts that are run to keep everything properly aligned. • Weeding for Scottish arrests is determined by Scotland's Criminal History System, in line with Scottish regulations, which informs PNC - which in turn instructs IDENT1 which records to weed. • Weeding for Northern Ireland arrestees is determined by their Biometric Retention and Deletion system (which again informs PNC and onwards to IDENT1). • IDENT1 executes weeding requests on receipt from PNC. • Records can also be deleted by manual action - for example if an individual request has been made to a Chief Constable to remove a particular person's record. • Scene of crime marks are weeded by a semi-automated process as a decision needs to be made whether to retain or not (those of interest will have retention periods and reviewed in

	line); for example a murder case image could be kept indefinitely, and other images may be archived if no interest. This is in line with PoFA legislation.
5.4 What are the risks associated with how long data is retained and how they might be mitigated?	Retaining data beyond periods specified in the HOB Data Retention policy may lead to a breach of the Data Protection Act and PoFA. In principle, raw biometric images are not persisted on Matcher. All identity information (biometric and biographic) is mastered in IDENT1. Raw biometrics are initially sent to the Matcher from IDENT1 in order for the MES to carry out the initial encoding. These are not retained after the template is generated. Images are encoded into templates by the matching algorithm (provided by the MES) in a one-way function that redacts the image into the key machine-recognisable points used for matching. This is non-reversible and cannot be then used to reverse engineer a human-recognisable image. Design requirements state that temporary images must be deleted. Precise details of how deletion is achieved will be agreed with the successful supplier. The design incorporates layered security controls to prevent unauthorised access to the matcher and any subsequent data egress. There are no connections to Internet or other un-trusted networks. The NFRs further state that all storage media must be securely destroyed by an approved supplier when at end of working life.
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, this is a technical change to the matching process and does not affect subject access requests.
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.	There will be no Business user access to the Matcher Platform, Service Bus, Engine, or Algorithm[5]. There will however need to be appropriate supplier access to operate and maintain the system. There is a Security Architecture for HOB Biometric Services Platform; and a security

[5] Analytics may be accessed by Business support function

	architecture for each of the strategic projects. Procurement rules will also specify requirements to ensure that system access only by security personnel, to the appropriate level, as agreed with the Authority. The Service Supplier will be allowed access to a control panel that allows tuning of the algorithms and allocated processors etc. System administrators will manage and update the operating systems of the servers hosting the algorithm and platform. There will be the capability to mass migrate new collections into the matcher for new modalities and new algorithms. There is no access to manipulate biometric records. All levels of access will be specified in a role based access matrix with access controlled by Active Directory.
7.2 What level of security clearance is required to gain access to the system?	1. All Supplier Personnel who may have access to Police data or information systems must be cleared to NPPV3. 2. Any Personnel who have unsupervised access to the unencrypted Business Data will require minimum SC clearance. Approved, limited access for SC and NPPV3 cleared Personnel shall be supervised by a suitably cleared DBA.
7.3 Does the system use 'roles' to assign privileges to users of the system?	Yes
7.4 How is access granted to the system?	Role based access will be governed by Lightweight Directory Access Protocol, (LDAP). Controlled local accounts will be provided for authorised support purposes.
7.5 How are the actual assignments of roles and rules verified?	The project will provide a set of assurance documents to the Accreditor, including an Information Risk Assessment Report, supported by the Solution Security Design, SyOPs and IT Health Checks. Under Schedule 2.4 Security Management included in the Matcher procurement ITT there are requirements covering supplier access to the system. For example:- 1. Where the Supplier or Subcontractor grants increased IT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When Personnel no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1)

	Working Day. 2. The Supplier shall have auditable processes and controls in place for provisioning users, that limit access to ICT systems and estates used in providing the Services, such that access is only granted when absolutely necessary and only to authorised staff (whether Supplier or Subcontractor) who have appropriate authorised roles and vetting. 3. The Supplier shall implement Role Based Access Control (RBAC) for all users of the System, including system administrators. The RBAC shall be able to provide different access levels to systems and data. Roles may be based on job profiles, management grades, and team responsibilities. The principle of Least Privilege must be adhered to for all accounts. Access rights must be reviewed regularly and reported to the SWG via the monthly Security and Information Assurance Report. The Supplier shall retain an audit record of accesses for the Term of the contract. 4. The access control regime shall be compliant with ISO/IEC 27001 and ISO/IEC 27002, the Security Policy Framework, and the CESG IA Policy Portfolio.
7.6 How is this data logged and how is this reported to prevent misuse of data?	Protective monitoring including records of all access successful and failures. A Protective Monitoring Policy will identify the risk-based approached to monitoring, and the appropriate logs will be generated and collected by a Security Incident and Event Management system, for analysis by a professional Security Operations Centre. Additionally, all business transactions processed by the Matcher will be monitored and recorded in audit logs. The Chain of Evidence report, required for court cases as evidence of how someone's identity was confirmed, is existing functionality in IDENT1 Central which populates the report with information relating to an individual and their biometric and non-biometric information (including images). This information includes Ten Print forms, individual fingerprints and marks and audit information. This evidence will be unchanged by the new matcher. The matcher service will provide new audit information but this will not impact the chain of evidence which is managed by IDENT 1 Central system.
7.7 What training is provided to cover appropriate use and basic security to users? How is the training refreshed? Is the training tiered?	All HOB personnel receive security awareness training as part of their induction, both civil servants and contractors. All users must read and accept the POISE security operating procedures when first logging onto their account. The Department provides ongoing reinforcement training. Police users are subject to the IS awareness regime in their individual forces.
7.8 Has or is the system going to be	The Matcher falls under the purview of the HOB Security Working Group (SWG) which

formally accredited using HMG standards to process and store the information, if so who is the accreditation authority (person/organisation)?	provides active Information Assurance. HOB follows the Home Office risk discovery methodology and has adopted the Police Service Information Risk Acceptance Report (IRAR) as a means of capturing and communicating risks to stakeholders. The HOB Accreditor is a member of the SWG who will assess the Matcher IRAR and supporting documentation, making an acceptance recommendation to the Information Asset Owners.
7.9 Given access and security controls, what privacy risks were identified and how might they be mitigated?	The risk discovery process and workshops with NCSC identified a number of potential threats to images (temporarily) at rest and in transit to the Matcher. As a summary, the following were identified as key risks to the Matcher information and the service provided to its end systems/users across law enforcement, immigration, and HMPO. • System outage impacting a large number of operational use cases across Law Enforcement and government; if the Matcher is out of action, then front-end systems cannot enrol, search or update biometric records which is a major risk. • Integrity issues affecting match results and the decisions that are made as a result; users of the system may be coerced or bribed to misuse their access and help someone bypass the visa or law enforcement system by making unauthorised changes to the records (additions, removals, modifications). Motivations for this could include financial/bribery, activism or coercion. Here there is some mitigation in that most decisions which have an impact on people's lives have a human involved rather than being entirely automated. • A user being able to search records and get a result from a collection that they are not authorised for i.e. going on 'fishing trips'. The Security NFRs and Matcher incorporate requirements to mitigate these threats. As noted earlier, the images being converted into templates by matcher do not have any meta data that would allow the subject to be identified without access to further data that is not held in Matcher.
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?	Not by this project – sharing is done from IDENT1 Central as part of business as usual and is unchanged by the matcher project.
8.2 If you will be making transfers,	n/a

how will you ensure that the data is adequately protected?	
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?	The project does not share data as such; the results of the fingerprint matching will be returned automatically to the IDENT1 system. The results may be subsequently shared by the police for public protection purposes.
9.2 How is the information processed or disclosed?	As stated the results of the fingerprint matching will be returned automatically to the IDENT1 system and the match results presented (match..no match).
9.3 What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?	The project is not responsible for data sharing and this remains with the data controller/processor.
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?	The project does not share information with external organisations it provides a match/no match response to IDENT1 Central to distribute to the requestor (Police or Immigration).
10.2 Is the sharing of personal information outside the Home Office compatible with the original collection? If so, is it addressed in a data-sharing agreement? If so, please describe.	This project will deliver an engine to perform a technical process and does not share information. However, the results of the match may be shared by the Data owners under a legal framework, for example, for policing purposes Section 63T of the Police and Criminal Evidence Act 1984 (http://www.legislation.gov.uk/ukpga/1984/60/section/63T) allows DNA and fingerprints to be used to prevent and detect crime inside or outside England and Wales. Similar provisions apply in Scotland and Northern Ireland. Or for immigration purposes under the Immigration Acts.
10.3 How is personal information shared outside the Home Office and what security measures, compliance, and governance issued safeguard its transmission?	The project is not responsible for data sharing and this remains with the data controller(s)/processor(s).
10.4 Is a MoU in place for the Home Office to verify that an external	The project is not responsible for data sharing and this remains with the data controller(s)/processor(s).

organisation has adequate security controls in place to safeguard information?	
10.5 Given the external sharing, what are the privacy risks and how might they be mitigated?	The project is not responsible for data sharing and this remains with the data controller(s)/processor(s).
Notice	
11.1 Do individuals have an opportunity and/or right to decline to disclose or share information?	Not within the remit of this project which just processes the information but in general the information is required, under PACE[6] and individuals do not have the right to decline.
11.2 Do individuals have an opportunity to consent to particular uses of the information, and how?	n/a
11.3 How could risks associated with individuals being unaware of the collection be mitigated?	n/a
Access, Redress and Correction.	
12.1 How are individuals notified of the procedures for correcting their information?	Linking back to biographical information is outside the scope of this project Outside of this project procedures are in place to correct biographical errors.
12.2 If no formal redress is provided, what alternatives are available to the individual?	Outside of this project formal redress is available. In line with published procedures subjects can have their information removed from the police databases which would result in a removal of the template from Matcher.
12.3 What are the privacy risks associated with redress and how might they be mitigated?	n/a
Aggregation of Data	
13.1 Will the wider sharing or aggregation of data held pose a risk of injustice to groups or individuals?	No. The Matcher platform is a single component which plays a role in HOB end-to-end services. Matcher holds no personal information, only biometric data, and associated metadata. At this point only Law Enforcement records will be included in the Matcher, and at a later point it is intended to physically locate templates from other Lines of Business including HMPO and Immigration. This will be subject to discussion and approval with the appropriate stakeholders.

[6] Some fingerprint sets are volunteered for elimination purposes.

	The wider HOB programme PIA will address this.

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

Annex A

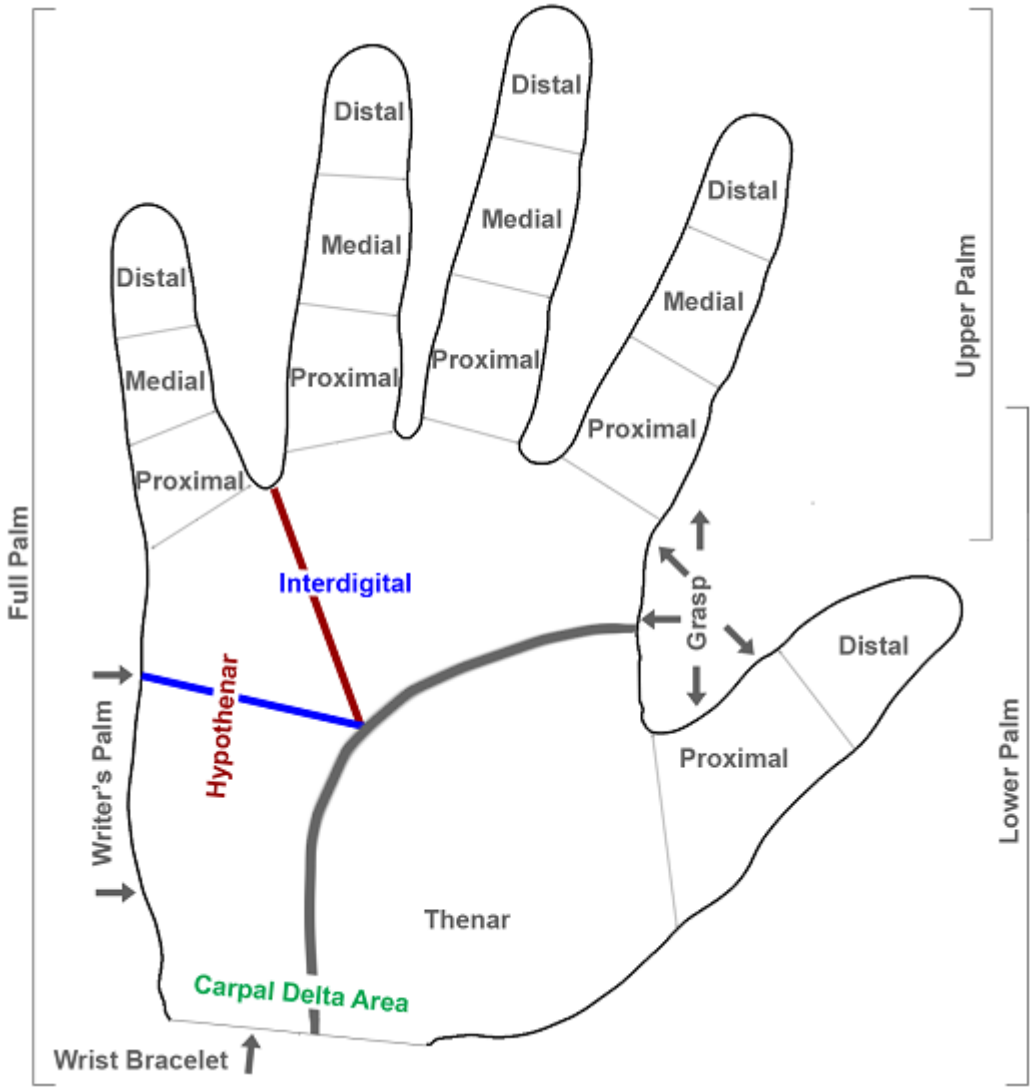
Official – sensitive: start of section

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

Official – sensitive: end of section

Annex B

NIST fingerprint standard – Diagram
Palm and finger segment positions



ANSI/NIST-ITL 1-2011 Update:2015