Home Office Biometric Programme - Privacy Impact Assessment – Latent Mark searches on immigration data

This PIA was agreed on 9th March 2018

PIA Initial Screening Checklist
Programme/project/policy: The adhoc searching of latent marks from specialist bureau against immigration data will become available from Q1 2018. The changes to the **Immigration and Asylum Biometric System (IABS)**, in Release 10, were completed in November 2017, with **IDENT1 (Law Enforcement and Security Biometrics System)** changes due to be completed and tested by Q1 2018. The adhoc search capability will speed up the identification of immigration and crime offenders and provide an increased capacity to use this biometric identification method. The current process is capped at 100 cases per week (although actual volumes are much less) due to the manual nature of the process which requires Immigration Fingerprint Bureau (IFB) staff to load the latent mark searches and check the results. The new automated functionality will increase the volume capacity, by exploiting some capacity that was not being fully used, to an average of **380 (max)** latent mark to print searches per day, with a peak hour capacity of 54. • The Home Office is Data Processor for information held on IDENT1 • The Home office is Data Controller and Data Processor for information held on IABS.

- Chief Constables are all data controllers for the fingerprint marks and DNA samples collected within their force. The Chair of the Forensic Information System Databases Strategy Board (FIND SB) is the data controller in common

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 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:			

Official – sensitive: start of section

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

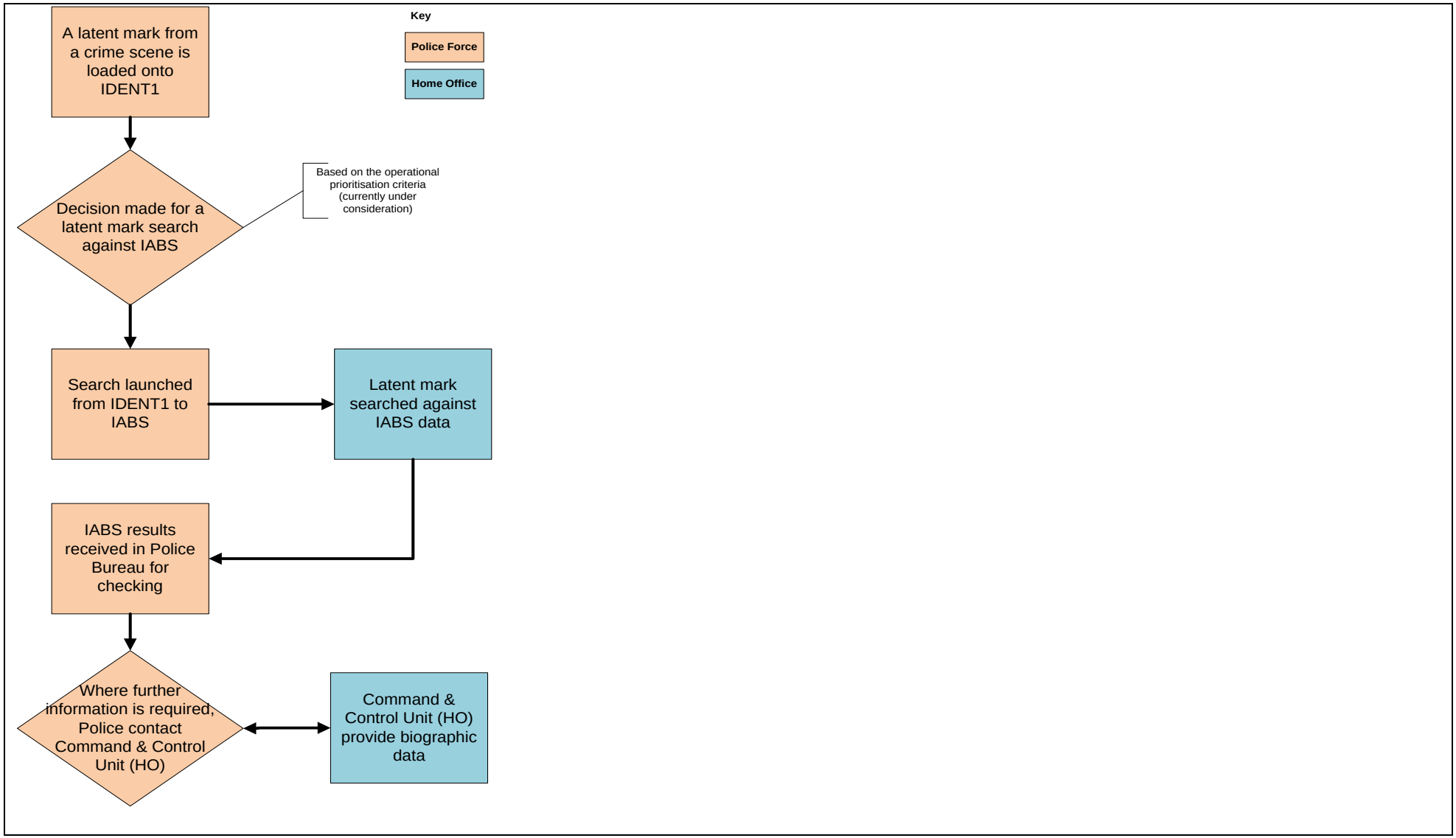
Home Office Privacy Impact Assessment
Identify the need for a PIA: Explain what the project aims to achieve, what the benefits will be to the Home Office, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. 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 completion of the developments to IABS and IDENT1 by Q1 2018 will make it possible for latent mark searches to be launched directly against IABS from the IDENT1. For the first period of live running of this service searches will only be allowed from two specialist law enforcement departments **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** This will move the current, largely manual, matching process, to an automated one where specialist bureaux can search directly against IABS database with the benefits including: • Increased capacity of fingerprint checks. The current process is capped at 100 cases per week due to the manual nature of the process which requires IFB staff to load the latent mark searches and check the results

- Producing more matches from crime scene marks, providing the police with more information to support their investigations of crimes.
- Speed up identification of immigration and crime offenders
- Free up resources in the UKVI Immigration Fingerprint Bureau as there will be less need for physical checks made by IFB staff. Where automated, the checking of results will be conducted by the specialist bureau

This automated service may be expanded at a later date to general policing but would require a further change to IDENT1 to enable this and some quota management functionality.

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.

The data flow will be simplified through the automation of the matching process. A high level (draft) flow chart is as follows:


Key
Police Force
Home Office
A latent mark from a crime scene is loaded onto IDENT1
Decision made for a latent mark search against IABS
Based on the operational prioritisation criteria (currently under consideration)
Search launched from IDENT1 to IABS
Latent mark searched against IABS data
IABS results received in Police Bureau for checking
Where further information is required, Police contact Command & Control Unit (HO)
Command & Control Unit (HO) provide biographic data

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.

For this paper, consultation has been limited to:

- HOB Biometric Architect
- HOB Technical Architect
- UKVI IFB
- Immigration & Border Policy Directorate
- HOLA
- CPFG Policy

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?	Latent marks are collected for the purposes of investigating crime Fingerprints held on IABS are collected for immigration purposes
1.2 Where is the information collected from, how, and by whom?	Latent marks are collected at crime scenes. They are impressions of friction ridge detail left on surfaces that are not visible and require going through a visualisation process (e.g. dusting or chemical treatment) before they can be seen The immigration purposes for which fingerprints are taken and held on IABS are outlined below in 1.8
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?	Chief Constables are all data controllers for the fingerprint marks collected within their force. The Chair of the Forensic Information System Databases Strategy Board (FIND SB) is the data controller in common The Home Office is Data Processor for information held on IDENT1 The Home office is Data Controller and Data Processor for information held on IABS.
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?	Individuals who give their biometrics for immigration purposes are informed at the point of collection that their data will be used by other agencies for the purposes of criminal investigations and national security

1.5 Have you established which conditions for processing apply?	Latent marks are collected through crime scene investigations and the images of fingermarks are held on IDENT1. Following Release 10 in IABS in November 2017 and the delivery of IDENT1 changes (including testing) by Q1 2018, two specialist law enforcement departments **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** will be able to make a search directly from IDENT1 into IABS for the latent mark
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 policing process does not rely on consent.
1.7 What information is collected, used, disseminated, or maintained in the system?	Latent marks collected at a crime scene will be searched against the IABS database. The match result will automatically be sent back to the bureau making the search The unconfirmed result that is returned to IDENT1 will contain the biographic data held on IABS for the unconfirmed match and a photo image. The bureau will review the results to confirm the matches and discount the no matches
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?	The following sections in **Part II (Powers of entry, search and seizure) of the Police and Criminal Evidence Act 1984 (as amended)** apply to the recovery and retention of latent marks: **s.8** provides for a warrant to be issued by a justice of the peace if; there are reasonable grounds for believing that an indictable offence has been committed and it is believed that a

	premises contains evidence of substantial value to an investigation that is likely to be relevant and admissible **s.19** confers the powers to a constable, when lawfully on a premises (i.e. without a warrant), to seize any evidence from the premises where there are reasonable grounds for believing that it can be used in the investigation of the offence being investigated or any other offence **s.22** outlines the retention periods for items seized under s19 **The Immigration (Biometric Registration) Regulations 2008**, as amended, and the **Immigration (Provision of Physical Data) Regulations 2015** which amends the Immigration (Provision of Physical Data) Regulations 2006, are secondary legislation covering the collection use and retention of biometrics for immigration purposes – including requiring all non-EEA nationals applying for leave of over six months to apply for a biometric residence permit (BRP), those applying for leave to enter or remain in the UK, those applying for indefinite leave, those making claims for asylum, and those applying in-country for replacement immigration documents. During the process of application, an authorised person may require the applicant to provide a record of their fingerprints or photograph of their face. The Regulations set out that the Secretary of State may retain biometrics provided in connection with an application where she thinks that it is necessary to retain it for use in connection with: • the exercise of a function by virtue of the Immigration Acts or in relation to nationality; However, she may also use these retained biometrics: • in connection with the prevention, investigation or prosecution of an offence; • for a purpose which appears to the Secretary of State to be required in order to protect

	national security; • in connection with identifying persons who have died, or are suffering from illness or injury; • for the purpose of ascertaining whether a person has acted unlawfully, or has obtained or sought anything to which the person is not legally entitled; and • in connection with the exercise of a function concerning the entitlement of a person who is not a national of an EEA state or Switzerland to enter or remain in the United Kingdom by virtue of an enforceable EU right or of any provision made under section 2(2) of the European Communities Act 1972(1). Fingerprints will normally be retained for up to 10 years so long as the Secretary of State believes that they are required for the purposes above. However; fingerprints may be retained beyond ten years where: • the fingerprints are of a person who is, or at any time has been, subject to a deportation order, exclusion order or decision to exclude; • the fingerprints are of a person who can be, or at any time could have been, refused entry clearance or leave to enter for a period specified in the immigration rules because of a previous breach of the United Kingdom's immigration laws; • the Secretary of State deems it necessary for national security reasons to retain the fingerprints for use in connection with one of the functions specified in regulation; • the fingerprints are of a person with indefinite leave to enter or remain in the United Kingdom; • the fingerprints are of a person whose indefinite leave to enter or remain in the United Kingdom lapses, is revoked or is cancelled, in which case they must be destroyed by the Secretary of State at the end of ten years beginning with the date of the lapse, revocation or cancellation (as the case may be); or

	• the fingerprints are of a person who
	  ○ is not a national of an EEA state or Switzerland; and .
	  ○ is the holder of a document which recognises the right of permanent residence in the United Kingdom by virtue of an enforceable EU right or any provision made under section 2(2) of the European Communities Act 1972,
	in which case they must be destroyed by the Secretary of State at the end of ten years beginning with the date on which the holder ceased to enjoy the right of permanent residence.

1.9 Is there a specific business purpose that requires the use of this information?	For the purposes of investigating crime
1.10 Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?	There is a potential privacy risk with biographic details of individuals being returned to IDENT1 as an unconfirmed match. Following a review by the bureau, if the result is not then confirmed (i.e. a no match), the record is to be deleted. Only confirmed matches may be investigated further. It is also possible that individuals may be a confirmed match against a latent mark, with their biographic details shared with the police and yet are not directly connected to the crime being investigated. The Police Force will need to request further information as part of the investigation and building up the evidence case. They will phone Command & Control Unit (CCU) in the Home Office for more details of the individual's immigration history if required.
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?	Not directly as the new automatic functionality will not 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 between the police and the Home Office is a proportionate response to the problem of how to detect who has committed crimes.

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 matching results will go to the bureau for manual verification by fingerprint experts (depending on thresholds etc.) and could be used for evidential purposes
2.2 Have you identified potential new purposes as the scope of the project expands?	No, the project is only replacing a largely manual process with an automatic one. It will be for the Police Forces to make decisions to request a search of a latent mark against IABS, on a case by case basis, based on the operational priorities and capacity outlined by the Data Controller
2.3 Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?	There is a potential privacy risk with biographic details of individuals being returned to IDENT1 as an unconfirmed match. Following a review by the bureau, if the result is not then confirmed (i.e. a no match), the record is to be deleted. Only confirmed matches may be investigated further. It is also possible that individuals may be a confirmed match against a latent mark, with their biographic details shared with the police and yet are not directly connected to the crime being investigated. The Police Force will need to request further information as part of the investigation and building up the evidence case. They will phone Command & Control Unit (CCU) in the Home Office for more details of the individual's immigration history if required.
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 latent marks can vary, but the quality of the immigration data being searched against is of good enough quality to support the latent mark search.
3.2 Which personal data could you not use, without compromising the needs of the project?	The initiation of the matching process does not use any personally identifiable biographical data. Match results returned to IDENT1 do contain the biographic details and photo image held on IABS. The bureau will confirm the match, undertaking further investigations to develop an evidence case. Matches that are not confirmed are to be deleted by the bureau.
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?	The changes are only enabling automatic matching against IABS and will not amend the data
4.2 How are you ensuring that personal data obtained from individuals or other organisations is accurate?	The functionality does not obtain its own data
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?	The automatic process being implemented will be a search only request of the latent mark against IABS. No personal data will be stored on IABS. However the search request activity will be logged, will be kept for audit purposes and subject to IABS data retention rules.

5.2 Are you procuring software that will allow you to delete information in line with your retention periods?	Not as part of this release
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?	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 scene of crime mark could be kept indefinitely, and other scene of crime marks may be archived if no interest. This is in line with PoFA legislation. IABS data passed to IDENT1 as an unconfirmed match is to be deleted if, after review by the bureau, it is confirmed as a no match
5.4 What are the risks associated with how long data is retained and how they might be mitigated?	Privacy risks for latent marks are deemed to be low However biographic data from IABS is returned to IDENT1 as an unconfirmed match for the police bureau to undertake a review. Where a match is confirmed the police force will need to make further investigations to identify whether the individual concerned is linked to the crime being investigated. Where a match is not confirmed, the data is to be deleted.
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?	This is a technical 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.	The access control to both IDENT1 and IABS systems will not be altered with these changes
7.2 What level of security clearance is required to gain access to the system?	The access control to both IDENT1 and IABS systems will not be altered with these changes
7.3 Does the system use 'roles' to assign privileges to users of the system?	The access control to both IDENT1 and IABS systems will not be altered with these changes
7.4 How is access granted to the system?	The access control to both IDENT1 and IABS systems will not be altered with these changes
7.5 How are the actual assignments of roles and rules verified?	The access control to both IDENT1 and IABS systems will not be altered with these changes
7.6 How is this data logged and how is this reported to prevent misuse of data?	As now, all transactions monitored and recorded.
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 users must read and accept the 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 formally accredited using HMG standards to process and store the information, if so who is the accreditation authority (person/organisation)?	The project falls under the remit of the HOB Security Working Group (SWG) which provides active Information Assurance. For law enforcement projects and systems the HOB SWG works closely with the National Police Improvement Risk Management Team (NPIRMT) whilst the primary HOB Accreditor is a member of both the HOB SWG and NPIRMT.
7.9 Given access and security	The access control to both IDENT1 and IABS systems will not be altered with these changes

controls, what privacy risks were identified and how might they be mitigated?	
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 as part of business as usual and is unchanged by the new searching functionality
8.2 If you will be making transfers, how will you ensure that the data is adequately protected?	Not applicable for this project
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?	The project will be sharing data with the police and not internally within the Home Office
9.2 How is the information processed or disclosed?	The project will be sharing data with the police and not internally within the Home Office
9.3 What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?	The project will be sharing data with the police and not internally within the Home Office
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	The project will share information with the police and provides an unconfirmed match/no match

organisation(s) is the information shared, what information is shared, and for what purpose? Has the Home Office specifically asked suppliers to undertake PIAs?	response to the specialist bureau, which also includes biographic data and photo image held on IABS. Where there is a match and the police request further information on an individual, this will be through existing processes and protocols – through a phone request to CCU
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.	The results of the match may be shared by the Data Controllers under a legal framework, for example, for policing purposes as outlined above in 1.8
10.3 How is personal information shared outside the Home Office and what security measures, compliance and governance issued safeguard its transmission?	The project will share information with the police and provides an unconfirmed match/no match response to the bureau, which also includes biographic data and photo image held on IABS. Where there is a match and the police request further information on an individual, this will be through existing processes and protocols – through a phone request to CCU
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?	Where there is a match and the police request further information on an individual, this will be through existing processes and protocols
10.5 Given the external sharing, what are the privacy risks and how might they be mitigated?	There is a potential privacy risk with biographic details of individuals being returned to IDENT1 as an unconfirmed match. Following a review by the bureau, if the result is not then confirmed (i.e. a no match), the record is to be deleted. Only confirmed matches may be investigated further. It is also possible that individuals may be a confirmed match against a latent mark, with their biographic details shared with the police and yet are not directly connected to the crime being

	investigated. The Police Force will need to request further information as part of the investigation and building up the evidence case. They will phone Command & Control Unit (CCU) in the Home Office for more details of the individual's immigration history if required.
11 Notice	
11.1 Do individuals have an opportunity and/or right to decline to decline to disclose or share information?	Not as part of this process
11.2 Do individuals have an opportunity to consent to particular uses of the information, and how?	Not as part of this process
11.3 How could risks associated with individuals being unaware of the collection be mitigated?	Not as part of this process
12 Access, Redress and Correction.	
12.1 How are individuals notified of the procedures for correcting their information?	There are procedures in place to correct biographical errors on the IABS and IDENT1 systems.
12.2 If no formal redress is provided, what alternatives are available to the individual?	There are published procedures on how individuals can have their information amended or removed from the databases
12.3 What are the privacy risks associated with redress and how might they be mitigated?	Not applicable
Aggregation of Data	
13.1 Will the wider sharing or	There is a potential privacy risk with biographic details of individuals being returned to IDENT1

aggregation of data held pose a risk of injustice to groups or individuals?	as an unconfirmed match. Following a review by the bureau, if the result is not then confirmed (i.e. a no match), the record is to be deleted. Only confirmed matches may be investigated further. It is also possible that individuals may be a confirmed match against a latent mark, with their biographic details shared with the police and yet are not directly connected to the crime being investigated. The Police Force will need to request further information as part of the investigation and building up the evidence case. They will phone Command & Control Unit (CCU) in the Home Office for more details of the individual's immigration history if required. The aggregation of data would occur in the event of a match and the police force requests further details on the individual. However this would form part of the development of the evidence base for the case and will be within existing police guidance. **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**

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