Home Office Biometric Programme - Privacy Impact Assessment – Biometric Services Gateway

This PIA was agreed on 6th June 2017

PIA Initial Screening Checklist
Programme/project/policy: [Please set out whether the Home Office is the Data Controller for this work and if not then what roles does it have] **The Biometric Services Gateway (BSG) Phases 1&2** The Home Office Biometrics Programme has a responsibility to provide common biometric services across the Home Office and to external stakeholders. A key early deliverable is to provide a "common front door" into the legacy systems from which new capabilities can be delivered and services consolidated. The Biometric Services Gateway (BSG) is being created to provide this "front door" capability. BSG Phase 1&2 starts the process to replace the FCOS, IABS and IDENT1 Departmental Integrated Service (DIS) boxes. The DIS boxes are part of the legacy infrastructure for transforming and transferring messages between • IDENT1 (a scene of crime and fingerprints database used by law enforcement) • IABS (the Immigration and Asylum Biometric Service: a fingerprint database used for immigration). • FCOS BVS (UK Visas' Biometric Visas System, which handles the biometric searches required for the wider visas processing) At Phase 1, traffic between IABS and IDENT1 will be routed via the BSG. The three sets of DIS boxes cannot be decommissioned until Phase 2 of the BSG cutover when traffic between BVS and IABS will also be routed via the BSG and IVAC special collection responses will be sent directly to iShare by BSG. It is of note that removal of the IABS DIS box also has a dependency on the IPT programme's replacement of the BRP DIS box. The BRP DIS box is out of scope for the BSG project, but must be retired before the IABS DIS box can be

decommissioned; the migration of BRP to IPT is now underway.

Data Controller/Data Processor.

The Home Office is Data Processor for information held on IDENT1

The Home office is Data Controller for information held on IABS.

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.

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

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[1], IABS[2] & NDNAD[3] 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. The Biometric Services Gateway is one of the projects being delivered within this programme.

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

[2] 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

[3] 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)

There are two primary drivers for investing in the Biometric Services Gateway (BSG) within the HOB domain:

1. Deliver an enhanced capability making cross checking against immigration and criminal fingerprints an easier and more efficient process
2. Support the HOB programme objectives for continuity of service & cost reduction,

The **Biometric Service Gateway (BSG)** is a separate component and key enabler, without which the wider programme will not be able to deliver. It will form part of a number of end-to-end services when coupled with other systems such as, for example, Strategic DNA, Strategic Mobile and Prüm.

Historically the service, cross checking against immigration and criminal fingerprints, was built in response to demand and resulted in a variety of connections to IDENT1 & IABS routed through or supported by DIS[4] boxes. As part of the tech refresh **required** and a critical step in delivering the HOB programme vision the BSG will provide a single gateway through which biometric data will be received and sorted. The BSG will be delivered in two stages – the first will provide a **stable platform** through which the existing IDENT1 and IABS Data can be accessed. Subsequently it will provide the single point of entry through to common capability technology platforms.

Strategic DNA and Strategic Mobile and Prüm are in scope to interface with BSG and in due course will require this PIA to be updated; however, this PIA only concerns the BSG phases 1&2. In addition this PIA will not deal with privacy implications around the collection of biometrics but will look at privacy implications around the specific processing being carried out by the BSG phase1&2. The BSG PIA will be updated by those projects if required.

Implementing BSG (all phases) would be expected to bring the following benefits: [5]

[4] DIS (Departmental Integrated Service) boxes are part of the legacy infrastructure for transforming and transferring messages between IABS, FCOS IDENT1 etc

[5] Business case V0.7.2

1. De-coupled system components:
    a. This increases business agility by making change simpler (and thus cheaper, faster and lower risk)
    b. And enables individual components within the technology landscape to be updated / replaced with minimum impact on the remaining estate
- Clearer separation of responsibilities.
- Increased re-use, reducing cost to implement future changes, additional biometrics modes, etc.
- Provides standardised messaging capability (including aspects such as any guaranteed delivery need, security model, message format translation etc.), again reducing costs and enhancing consistency.
- Enables the legacy DIS capability to be retired.

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.

Collection of data is not the remit of the BSG. Data is collected by external systems which are covered by their own PIAs. The BSG facilitates the exchange of data between those external systems. In doing so, the BSG supports a range of end to end biometric business processes, such as visa enrolments, asylum applications, biometric residency permits, international data sharing, criminal police searches and so on, by routing biometric data between and on behalf of those external systems.

BSG does not retain any personal information for purposes other than to deliver it. Once data is delivered, personal information is redacted from any persisted data such that only transactional meta-data is retained for audit purposes. BSG stores meta-data (data about data), for the purpose of tracking transactions. This data can then be retrospectively used for reporting, problem diagnosis, and chain of evidence. The meta-data includes items such as timestamps, transaction identifiers, the systems involved, record identifiers, and transaction types. There is no personal information. Whilst some of the data could be used to identify a record in another system, that other system would have to be accessed first.

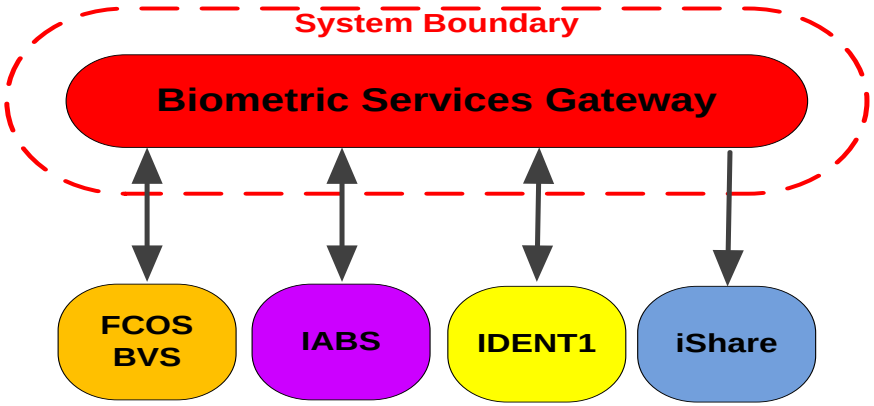
BSG obfuscates any personal information (biographic and biometric data) through the use of hashing. BSG hashes the information which is to be redacted. This hash cannot be reverse engineered to re-create the original data. It is a one-way process. However, in the event that data needs to be compared, for example if it were necessary to take a request from another system and demonstrate that it had been processed by the BSG, the data to be compared can be hashed with the same algorithm and compared to the data

audited in the BSG, to show that they are the same.

The diagram below presents the context of the BSG in the wider technical estate:

BSG as a system, by itself, does not specifically deliver any complete business services. Rather, it is a layer within HOB which, when used with other layers (Central, Matcher, etc), provides a number of vertical services to different business capabilities (Mobile, Prüm, DNA, etc).

No new individuals will be affected by the BSG project, as at this phase it is essentially a replacement for existing capabilities. The introduction of the BSG will be transparent to existing services.



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 the HOB EG. The BSG PIA will form part of the overarching HOB PIA and submitted with the HOB PIA.

The SRO for the Biometric Service Gateway has been consulted with from the outset of the project. Project Governance is provided through:

HOB Programme Board

HOB Programme Investment and Appraisals Group (PAIB)

HOB Programme Alignment Working Group (PAWG)

BSG Project board

HOB Security Working Group (SWG)

BSG Security Working Group informing HOB SWG

In addition IDENT1 Users along with others have been consulted at the design phase where high level requirements and benefits were identified. This included the identification of non-functional requirements related to privacy. This information has been carried over into the elaboration phase of the project, where stakeholders continue to be consulted. The project went live 21st January 2017

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 Biometric Services Gateway does not collect – it transports data between external systems
1.2 Where is the information collected from, how, and by whom?	In certain circumstances specified by law fingerprints may only be taken for the purpose of verification (to confirm that an individual is who they claim to be or to confirm whether an individual has previously had their fingerprints stored). The BSG transports data collected by police and Immigration using powers set out in the Acts mentioned below (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 overseas.
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?	BSG does not collect information. It deals with personal data by restructuring it and transferring it. The data is collected by others under legal frameworks and relationship as set out in 1.8 **Home Office as Data Controller** Where the data is collected by others on behalf of the Home Office, the Home Office is Data Controller. For example there is a formal agreement with FCOS, (commercial partner for overseas collection of biometrics) as data processor, via commercial contract. **Home Office as Data Processor** Where the Home Office is processing the data on behalf of others, the Home Office is data processor. This activity takes place only when there is a formal agreement for example a commercial contract or MOU in place.

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?	The BSG does not inform individuals about the use of the personal data. However processing notices apply to the collection of biometrics (by others) that will be transit the BSG.
1.5 Have you established which conditions for processing apply?	BSG does not process – there is no decision logic within BSG to decide which applications to process
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, in most instances, rely on consent. However, where fingerprints are enrolled for vulnerable persons, consent is required.
1.7 What information is collected, used, disseminated, or maintained in the system?	BSG does not collect data; the BSG disseminates data so that the different systems can consume it. The system forms a one way hash of the biometric and biographic data contained in the message. Hashing is an industry standard for obfuscating data such that it can still be compared to the original, without being able to derive the original from the hash. The redacted message is stored with transactional meta data. As per the BSG data retention policy for 30 days the data is stored within the system, then, for 7 years data it is stored in archives.
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	Not applicable to BSG itself however data is collected under powers as set out below: Relevant powers

merely permit it?	1) For policing purposes – policing is a devolved matter so separate Acts apply: England & Wales • Police and Criminal Evidence Act 1984 Scotland • Criminal Procedure (Scotland) Act 1995 Northern Ireland • Police and Criminal Evidence Act (Northern Ireland) Order 2013 Guernsey & Channel Islands **Under PACE Police have powers to share with others (for example immigration)** 2) For Immigration purposes – immigration is not devolved Fingerprints and facial images required for immigration purposes are collected under The Immigration and Asylum Act 1999 and regulations made under: • The Nationality and Immigration Act 2002 (as amended), • The UK Borders Act 2007 (as amended) & • The British Nationality Act 1981 (as amended). • The Immigration Act 2014 (Aligned immigration powers around retention and use of biometrics).

1.9 Is there a specific business purpose that requires the use of this information?	Law enforcement and immigration – this covers a wide range of business purposes.
1.10 Given the amount/type of data collected, what are the privacy risks? How they might be mitigated?	Privacy risks are around data integrity and data confidentiality. When data is transferred to the BSG it is signed which gives assurance of the integrity, i.e. that the data has not changed. The data is also encrypted so anyone intercepting the message cannot see it. Internally, data is managed in a secure government accredited data centre. All data is transient with the exception of the audit data base in which all personal biographic/biometric data is redacted.
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 end-to-end processing of police and immigration will interfere with privacy rights in Article 8 The project is designed to enable more effective processing which will enable more crimes to be detected and better immigration control. It is necessary in a democratic society to present and detect crime and to apply appropriate immigration controls. Therefore enhanced matching which will be provided by the BSG is a **proportionate response** to the social need.
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?	Not applicable - BSG just transfers information from one authorised system to another– transforming it where required. From an end-to-end perspective, the information passing through the BSG will relate to the control of immigration and the prevention and detection of crime.
2.2 Have you identified potential new purposes as the scope of the project	No. The scope of the BSG is an extensible platform, which will onboard additional systems and

expands?	whilst those systems are known the detail of the mechanics are to be determined. However Business needs, not the BSG, will be the driver for these new systems and interfaces.
2.3 Given the sensitivity and scope of the information collected, what privacy risks were identified and how might the security controls mitigate them?	A risk around aggregation of personal information in the audit store was identified. This is mitigated by hashing out the biometric and biographic data within the messages. The hashing algorithm is unidirectional in that the resulting hash cannot be used to reengineer the original data.[6]
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 BSG scope to define what is collected and quality checks are done within the user Bureau (outside of the BSG scope).
3.2 Which personal data could you not use, without compromising the needs of the project?	None because the obligation for the BSG is to deliver the complete data set provided from external systems to the recipient system.
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 BSG transforms and restructures data to be transmitted to its destination, but it does not amend the personal data.

[6] Hashing is the technical anonymisation of data

4.2 How are you ensuring that personal data obtained from individuals or other organisations is accurate?	The original collection of the data is subject to data quality rules which the user undertakes at the endpoint; extensive testing has demonstrated that BSG ensures accuracy is maintained.
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 BSG does not store personal data. Biometric data that traverses the BSG does include both biographic and biometrics. However as stated above an audit trail is retained in line with the BSG data retention policy -30 days online and 7 years off line. BSG does store information about transactions made. This is transactional and does not contain personally identifiable information. However: For police purposes the Protection of Freedoms Act 2012 (PoFA), which amended PACE, established a new regime to govern the retention and use in England and Wales of DNA samples, DNA profiles and fingerprints taken by the police. This also happens under the Scottish system which was the model for the regime set out in PoFA For immigration purposes fingerprints (and facial images) required for immigration purposes are collected under The Immigration and Asylum Act 1999 and regulations made under: • The Nationality and Immigration Act 2002 (as amended), • The UK Borders Act 2007 (as amended) & • The British Nationality Act 1981 (as amended).

5.2 Are you procuring software that will allow you to delete information in line with your retention periods?	Yes – standard database tooling. Also end of life storage media is destroyed.
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?	BSG does not store/retain any personal data.
5.4 What are the risks associated with how long data is retained and how they might be mitigated?	BSG does not store/retain any personal data, where messages are queued until delivery, these messages are susceptible to being accessed by Administrative personnel. Mitigations in place include: • Personnel security vetting – SC and NPV3 • SIEM (Security information and event management) – protective monitoring on use of administrative privileges.
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?	Not applicable
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.	BSG does not typically enable access to users as it is designed to provide system to system communication. Only support personnel are provisioned with access to the system based upon their role (i.e. Level 2 support or Level 3 support) that also requires security vetting described further below.
7.2 What level of security clearance is required to gain access to the system?	Support access to BSG requires security vetting to Security Check (SC) and Non-Police Personnel Vetting (NPPV) level 3.
7.3 Does the system use 'roles' to assign privileges to users of the system?	Yes see 7.1
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 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.
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 (for example selecting and maintaining high quality passwords, adhering to cyber security policies, protecting personal data, and avoiding potential sources of infection). 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.
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)?	BSG has been granted accreditation 2017 by the National Policing Accreditor.
7.9 Given access and security controls, what privacy risks were identified and how might they be mitigated?	The BSG does not store personal data. Where messages are queued until delivery, these messages are susceptible to being accessed by Administrative personnel. Mitigations in place include: • Personnel security vetting – SC and NPPV3 • SIEM – protective monitoring in use that also reports on administrative privileges.
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?	Yes BSG transfers data to FCOS BVS (UK Visas' Biometric Visas System, which handles the biometric searches required for the wider visas processing).
8.2 If you will be making transfers, how will you ensure that the data is	All delivered to the Home Office. FCOS delivers services via MOU (external supplier)

adequately protected?	
Internal sharing within the Home Office	
9.1 With which part of the Home Office is the information shared, what information is shared and for what purpose?	BSG is a conduit through which other parts of the HO share information. It facilitates confirmation of delivery.
9.2 How is the information processed or disclosed?	The BSG is the technical means by which data sharing arrangements are implemented, and the governance arrangements are put in place prior to any impact on the BSG. The BSG assumes that the governance is in place and does not introduce any new data sharing arrangements
9.3 What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?	Not applicable to this PIA, this is addressed within the wider Programme PIA
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 Data owners agree sharing, subsequently the sharing is facilitated by BSG
10.2 Is the sharing of personal information outside the Home Office	See 10.1

compatible with the original 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 to BSG However MOU and ISA are in place when information is shared outside of the Home Office
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 to BSG
10.5 Given the external sharing, what are the privacy risks and how might they be mitigated?	Not applicable
Notice	
11.1 Do individuals have an opportunity and/or right to decline to decline to disclose or share information?	Not applicable / visible to BSG; this covers engagement with the end user which is out of the scope of the BSG.
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
Access, Redress and Correction.	
12.1 How are individuals notified of the procedures for correcting their information?	Not applicable
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
Aggregation of Data	
13.1 Will the wider sharing or aggregation of data held pose a risk of injustice to groups or individuals?	No BSG is a single component which plays a role in a number of wider end-to-end services, built from many systems. As this PIA is specifically targeted at BSG, then it is not applicable; BSG holds no personal information. The wider HOB programme PIA will address this.

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? Please give details of appended Risk Register.

The next BSG PIA will be Lessons Learned.

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