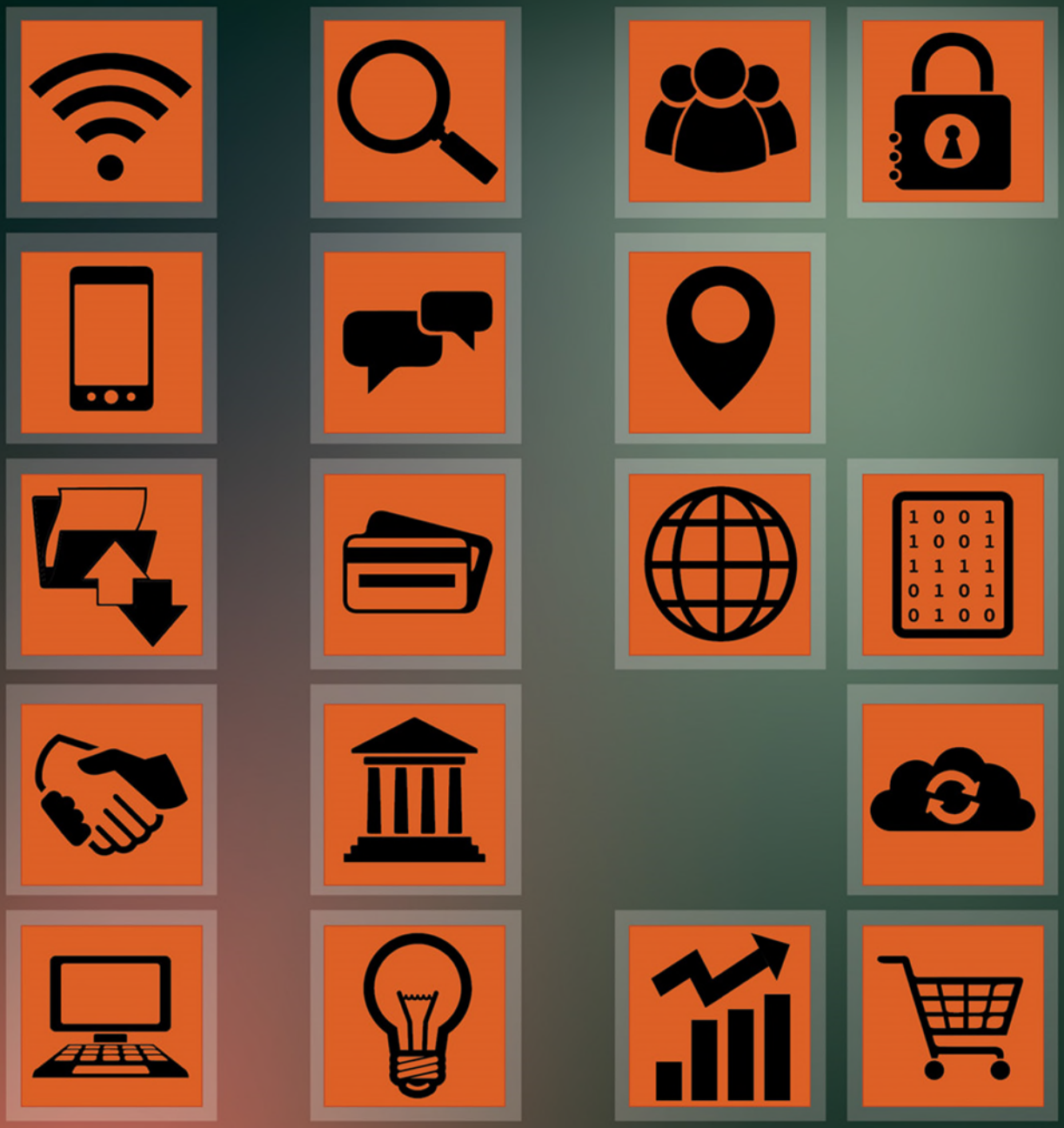


National Facial Biometric Matching Capability

Privacy Impact Assessment – Interoperability Hub

For: Attorney-General's Department

Date: August 2015

INFORMATION INTEGRITY SOLUTIONS

managing the **privacy** of **individuals** is **complex** and we can help you get it **right**

Table of Contents

1. Executive Summary

The Attorney-General's Department (AGD) engaged Information Integrity Solutions Pty Ltd (IIS) to undertake a privacy impact assessment (PIA) during the early design stage of the Central Interoperability Hub (the Hub) of the forthcoming National Facial Biometric Matching Capability (NFBMC). IIS has not been asked to assess or comment on the potential privacy impact of the concept of the NFBMC as such, or its overall operation. Rather, IIS has been asked to focus its findings on the Hub design and its initial operation and governance, taking account of the NFBMC's vision and aims.

Government agencies are increasingly using facial biometric systems for a range of law enforcement, national security and identity assurance purposes and in these contexts are sharing biometric information. However, the current arrangements tend to be ad hoc and limited by legal or technical incompatibilities.

The NFBMC is intended to facilitate secure, accountable sharing of facial images and other relevant information to prevent fraud, support law enforcement, promote national security, and streamline service delivery. Subject to inter-governmental and inter-agency agreements, the Hub will transmit facial biometric and biographic information between participating agencies in compatible formats. The Hub is intended to be 'neutral' – participating agencies remain responsible for their information, the application of biometric technologies and decisions about whether or not images match. The Hub will store some transaction metadata but does not store any of the biometric or biographic information it transmits.

Biometric information is widely considered to be intrinsically sensitive and agencies' use of biometric matching techniques, if not well managed, could cause significant problems for individuals through mismatches, stigmatisation and inability to gain easy redress.

IIS welcomes AGD's approach of undertaking a PIA at this early stage in the development of the NFBMC and of adopting Privacy by Design (PbD). PbD is based on seven principles which include 'Privacy Embedded into Design' and 'End-to-End Security'. The application of these principles in this case have resulted in decisions to adopt the hub and spoke architecture and for the Hub to store minimal information.[1]

This PIA focuses on only one element of the NFBMC. Its scope is limited to the Hub design and governance. AGD indicates that all Commonwealth, State and Territory participating agencies will be required to undertake further PIAs that focus on their use of the NFBMC as it develops. These would address, for example, participating agencies use of the Hub and the proposed driver licence facial recognition solution.

This PIA analysis recognises the steps AGD has taken so far to minimise privacy risks and to design-in strong security measures. It also takes account of the benefits that the Hub could deliver, including in addressing identity fraud and theft, which is having an increasing impact on individuals.

[1] See https://www.privacybydesign.ca/

At the outset, IIS considers that it is important to recognise that the Hub will have an impact on the circumstances in which facial biometric information is shared, by whom and the volume of images shared, and these risks will have to be actively managed. There is also the risk, which IIS considers is low, that the Hub and the metadata generated by transactions performed through it could potentially allow for some tracking or surveillance of individuals' everyday activities. However, it is the view of IIS that the privacy impacts of the whole system could well be greater than the risks at individual agency or Hub level. As such, IIS considers that strong, widely respected governance of the system as a whole as, particularly as it evolves over time, is equally and potentially more important than governance of the individual participating agencies and the Hub.

1.1 Findings

IIS considers that AGD's approach to the Hub design process has been generally consistent with the requirements of the Australian Privacy Principles (APPs) in the *Privacy Act 1988*. IIS has not identified any significant risks or privacy issues in the Hub design. IIS has identified areas where it considers some extra steps are needed to maintain the focus on privacy and good privacy practice. These include:

- The ongoing management of privacy in the Hub design
- The metadata the Hub will generate about transactions
- The Hub access and security arrangements.

IIS also considers that AGD's approach to the Hub's operation and the likely governance arrangements is also consistent with the APPs and it has not identified any significant compliance risks. IIS has made a number of recommendations to strengthen privacy practices. These recommendations take account of the multi-jurisdictional nature of the NFBMC and aim to promote continued privacy good practice to help ensure the aspiration of 'robust privacy safeguards' is delivered. The areas in which IIS considers there are potential privacy risks include:

- The scope of the NFBMC
- AGD's privacy management framework for the Hub
- The extent to which the development and operation of the Hub is conducted openly and transparently
- The NFBMC Governance arrangements including the governance of change.

1.2 Recommendations

1.2.1 Recommendations for Hub Design

1. APPs to apply to information the Hub collects, transmits or holds

IIS recommends that AGD in its role as Hub manager commit to complying with the APPs, whether or not the Hub is legally considered to collect or hold personal information.

2. Hub design informed by a broad view of privacy and the potential overall impact of the NFBMC

   (a) IIS recommends that AGD ensure that its further development of the Hub, and the governance arrangements for the operations of the Hub, reflect a broad view of the concept of privacy, as opposed to a strict legal compliance view.

   (b) IIS recommends that the Hub design and governance arrangements should, from the outset, take into account the Hub's likely future use, both in terms of the number and nature of participating organisations, as well as the volume and nature of information exchanged and the potential impacts on privacy.

3. Limit metadata to that needed for operational purposes and agency audits or investigations

   (a) IIS recommends that AGD ensure the metadata generated by the Hub is the minimum needed to:

      (i) Effectively manage the Hub

      (ii) Provide assurance that access to the Hub is for legitimate and appropriate purposes

      (iii) Ensure participating agencies can monitor their access to the Hub and undertake investigations of possible nefarious staff activities.

   (b) IIS recommends that the nature of metadata generated, and the period for which metadata will be retained be transparent to citizens.

   (c) IIS recommends that metadata generated by the Hub be retained for the minimum period needed to support the purposes for which it is generated.

4. Records of authority to release information

IIS recommends that AGD ensure the Hub design supports agencies' ability to make well-informed decisions to release images or biographic data based on a clear understanding of the purpose and authority for the request.

5. Strengthening of some security measures

   (a) IIS supports the access management approach proposed by AGD and recommends disabling and re-authorising all users and their level of authority at regular short, for example, three monthly intervals.

   (b) IIS supports the Hub project emphasis on training and standards and recommends that AGD ensure these address:

      (i) Appropriate personnel access to and use of the Hub

      (ii) Policy and procedures on the issue of image caching by agencies' online systems.

   (c) IIS recommends that AGD, in developing interagency templates, ensure they

      (i) Include strong controls for ensuring that only authorised individuals, cleared to Protected or higher as needed, can gain access to the system and only be authorised to undertake activity that reflects their level of authorisation

      (ii) Require the auditing of such access and provision of assurance about the appropriateness of access to biographic or biometric data to the holding agency.

6. Access to the Hub to identify individuals to be strictly controlled

(a) IIS supports the approach proposed by AGD and recommends that access to one-to-many matching be tightly controlled and limited to a few law enforcement agency uses (service delivery agencies should not have this access).

(b) IIS also supports AGD's general approach of limiting and controlling access to the Hub based on assessed risks in matching processes.

1.2.2 Recommendations for Hub operation and governance

7. Proactive privacy management

IIS recommends that AGD ensure that it has in place a privacy governance framework both to manage the Hub as it moves to BAU and when it is fully incorporated into BAU, which takes a broad view of privacy and commits to privacy best practice.

8. Benefits assessment to take account of privacy governance costs

(a) IIS recommends that in developing the methodology for identifying and costing benefits AGD and participating agencies should also bring into account all costs involved, including costs of privacy governance, such as:

(i) Participating agency compliance, and regular monitoring and audit costs

(ii) Resourcing of privacy regulators and other oversight bodies

(iii) Assistance to individuals and the community and complaint handling.

9. Project to be conducted transparently

(a) IIS recommends that AGD ensure that as soon as possible, and to the extent possible, information about the NFBMC and the Hub is in the public domain.

(b) IIS recognises AGD's intention to circulate and publish this PIA and recommends that it be published as soon as practicable.

(c) IIS recommends that AGD design and implement a proactive and transparent community engagement approach to support the introduction of the Hub.

10. Transparency in Hub use and intergovernmental agreements

(a) IIS recommends that all of the interagency agreements between participating agencies authorising information sharing via the Hub should be included in a register.

(b) IIS also recommends that the register be available for public inspection or that the interagency agreements are otherwise published and that all this documentation be easily available from the one source.

11. NFBMC scope

IIS recommends that AGD's documents and communications in relation to the NFBMC, including design specifications, undertakings and governance proposals, make clear the limits on the initial scope of the NFBMC. It must be made clear that if any change occurs in either the number or type of participating agencies, in the nature of the biometric and/or biographic information transmitted, or the

information held in the Hub, this would constitute a move beyond the initial scope and therefore trigger further privacy assessments.

12. The people's voice in governance arrangements

IIS recommends that the membership of governance bodies with a role in monitoring the operations of the NFBMC or in making decisions about changes in its scope or operations include an independent representative able to present individuals' perspectives.

13. Matters to be addressed in high-level intergovernmental agreement covering the NFBMC

(a) IIS recommends that the inter-governmental agreement that will set the framework for cross-jurisdictional sharing of biometric data via the Hub should:

(i) Ensure that privacy interests are appropriately represented on the body tasked with being accountable for the delivery and management of the Capability.

(ii) Require the receiving agencies to resource compliance audits by both themselves and the holding party or pay for independent audits to provide assurance to data holders

(iii) Require holding and receiving agencies to retain information that facilitates audits of the use of the Hub and regular systemic reviews of the system

(iv) Ensure resourcing for external oversight of the Hub by privacy regulators, Ombudsmen or anti-corruption bodies is commensurate with data flows and that there are no impediments to cooperation and information sharing between oversight bodies where information is shared between jurisdictions

(v) Require participating agencies to have in place well-resourced 'safety net' mechanisms to effectively support individuals who may be adversely affected by agencies' use of the Hub and to respond efficiently and respectfully to any complaints.

14. AGD or Independent approval of agreements between participating agencies

(a) IIS recommends that the Interagency Agreements between participating agencies, together with the IGA that will authorise information sharing via the Hub, should be subject to approval by AGD or by another independent body such as the Australian Privacy Commissioner before use of the Hub can proceed. If a body such as the Privacy Commissioner has this role, it should receive dedicated resourcing for this function.

(b) IIS further recommends that AGD take steps to ensure that the number of agreements does not reach the point where the sheer number adversely impacts transparency and community understanding of the system as a whole. These steps could include, as AGD is contemplating, standard agreements for groups of participating agencies or specifying the requirements in legislation rather than agreements.

15. Regular systemic review of the Capability and associated information sharing arrangements

(a) IIS recommends that there is at least a three-yearly systemic review of privacy impacts around the sharing of facial biometric information by participating agencies through the Hub. The findings of the review should be made public to the extent possible. The review should:

(i) Include the activities of the Hub and the participating agencies at both individual agency level and holistically

(ii) Quantify the increase in the use of facial biometrics amongst those agencies with legal authority to use the system

(iii) Quantify actual benefits realisation

(iv) Assess the extent to which the Hub itself is affecting privacy outcomes, including because the system performs less well than expected or has been subject to any significant data security breaches

(v) Assess the efficacy of responses to citizen issues with data accuracy and use, including but not limited to experiences with complaint handling

(vi) Assess the extent of community knowledge of the system, community reactions and impacts on privacy viewed broadly

(vii) Assess the effectiveness of the governance arrangements, particularly in relation to decision-making, oversight and accountability

(viii) Assess if the relevant oversight bodies are resourced for the functions and report if they are able to cooperate effectively.

16. Governance of changes to the Hub and associated information flows

(a) IIS recommends AGD, the National Identity Security Coordination Group or the Ministerial Law Crime and Community Safety Council, develop a governance process that would be triggered by any proposals that represent a significant change in the scope or operation of the Hub. The process should include:

(i) A broad consideration of costs as well as benefits

(ii) A commitment to a wide consultation process, including public consultations, to the extent possible

(iii) The inclusion of citizen perspectives beyond law, justice and national security agencies.

2. Introduction

The Attorney-General's Department (AGD) engaged Information Integrity Solutions Pty Ltd (IIS) to undertake a privacy impact assessment (PIA) during the early design stage of the Central Interoperability Hub (the Hub) of the forthcoming National Facial Biometric Matching Capability (NFBMC).

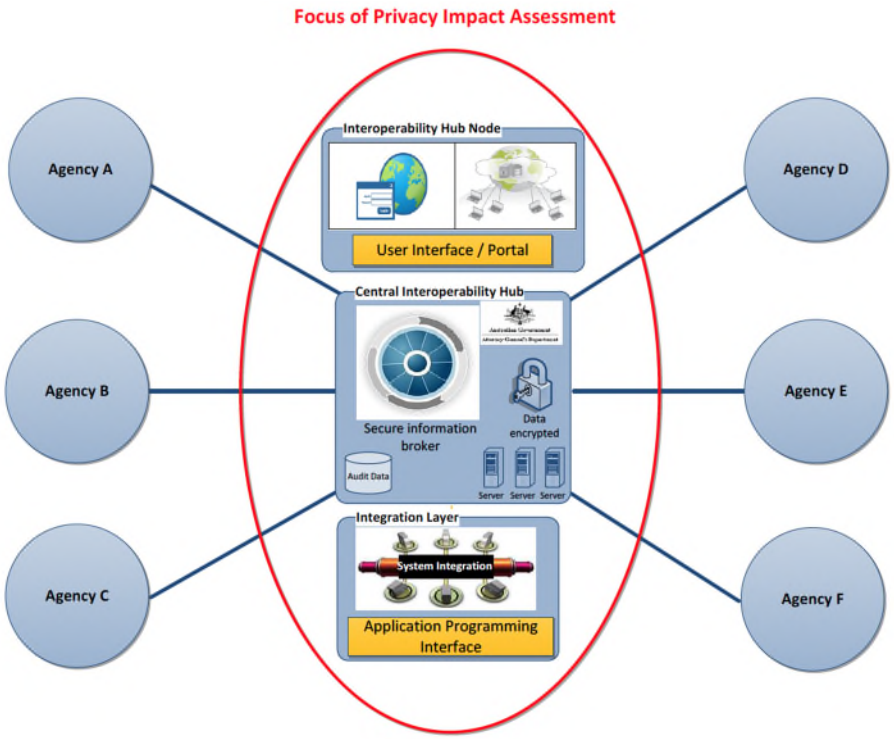
Government agencies, as well as private sector organisations, are increasingly using facial biometric systems for a wide range of purposes. These include supporting the issuance of identity credentials, such as passports and other documents that require a high level of assurance of a person's identity, and for law enforcement and national security investigations.

Agencies already share biometric information for these purposes and the amount of sharing is expected to increase, particularly in the context of strategies that seek to combat the increasing incidents of identity fraud in Australia. However, the current biometric sharing arrangements tend to be ad hoc and sometimes limited by legal or technical incompatibilities. The NFBMC is being developed to provide a practical means of increasing the interoperability of facial biometric systems used by Commonwealth, State and Territory government agencies. The Hub and associated arrangements are expected to facilitate secure, accountable sharing of facial images and other relevant information.

The Hub is currently at the design stage, with further design work to be informed by pilot activities that will shortly commence as well as this PIA and other investigations. The NFBMC is expected to commence its full rollout in 2016.

This PIA is an early stage assessment focussing on the Hub design and the potential privacy implications of information flows through the Hub (see Figure 1). IIS has not been asked to assess or comment on the potential privacy impact of the concept of the NFBMC as such, or its overall operation. Rather, IIS has been asked to focus its findings on the Hub design and its initial operation and governance, taking account of the NFBMC's vision and aims.

Figure 1: The Hub/agency relationships, and the focus of this PIA



It is out of scope for this PIA to consider agency activities the Hub might facilitate. However, the PIA does flag that ultimately the privacy impacts of the NFBMC will depend on uses to which the Hub is put and how that use is governed.

This PIA report provides background context, explores the possible privacy risks identified and makes a range of recommendations to address those risks.

2.1 Purpose and scope of the PIA

The NFBMC is a program of work comprising:

- The central interoperability Hub
- National driver licence facial recognition solution
- Legislative framework
- Standards and Training
- Governance.

This PIA focuses on the Hub and the related governance arrangements including the framework that will govern agencies' sharing of biometric and related information via the Hub. It involved:

- Identifying and assessing the privacy implications of the Hub, particularly in relation to the five core information flows

- Identifying any potential privacy risks and their impacts and recommending mitigation strategies that should be considered in the final design of the Hub.

The PIA did not extend to the collection, use and disclosure of personal information by Commonwealth, State and Territory agencies that will be participating in the NFBMC (in particular, the PIA has not considered the application of State and Territory privacy laws to agencies' participation in the NFBMC), the proposed national driver licence facial recognition solution, the legislative framework or the proposed standards and training.

IIS understands that these components will be subject to separate PIAs that AGD, or participating Commonwealth, State and Territory agencies, will commission.

2.2 IIS approach to the PIA

IIS prepared this PIA report taking into account the requirements of the *Privacy Act 1988* (Cth) (Privacy Act), in accordance with the *Guide to Undertaking Privacy Impact Assessments* published by the Office of the Australian Information Commissioner and drawing upon international privacy best practice approaches.

The PIA considers whether the Hub design and governance approach is consistent with the Australian Privacy Principles (APPs) in the Privacy Act. Importantly, and consistent with good privacy practice, it also considers broader privacy risks and Privacy by Design (PbD) issues that go beyond mapping specifically back to compliance with privacy law.[2]

The advice that IIS provides in this report is intended as strategic privacy advice. It is not intended as and should not be relied upon as legal advice.

2.3 Methodology

In undertaking this PIA, IIS took the following steps:

- Planned the PIA process in consultation with AGD
- Gathered information by:
  - Reviewing material about the context in which the Hub will be operating and the design of the Hub with a particular focus on the identified information flows including the high level solution design and functional and non-functional requirements (a full list of documents reviewed is at Appendix 1)
  - Holding detailed discussions the NFBMC Interoperability Hub Project team, the Australian Privacy Commissioner and State and Territory privacy commissioners, or nominated privacy representatives (for list of meetings with privacy regulators see Appendix 1)

[2] PbD is based on seven principles, which include 'Privacy Embedded into Design' and 'End-to-End Security'. Detailed information about PbD is available at https://www.privacybydesign.ca/.

- Analysed issues relevant to the design of the Hub taking account of the Privacy Act and broader privacy issues and the project approach
- Prepared its draft and final reports taking account of feedback from AGD.

2.4 Glossary

The glossary below sets out abbreviations, and definitions for key terms, used in this PIA. In line with AGD's approach, where the terms are generally used in the context of identity management policy IIS has relied upon the glossary prepared by the United States National Science and Technology Council's subcommittee on biometrics.[3]

Term or Abbreviation	Meaning or expansion
AGD	The Attorney-General's Department
Agency Request Reference	The participating agency transaction reference number
APPs	Australian Privacy Principles
Authentication	The process of establishing confidence in the truth of some claim. The claim could be any declarative statement for example: "This individual's name is 'Joseph K'." or "This child is more than 5 feet tall."
Biographic and Biometric content	The biographic and biometric information that is the *content* of the transmitted request or response and which is routed via the Hub between participating agencies
Biographic information	Identifying, or partial identifying information about an individual such as their name, date of birth, gender, address, place of birth
COAG	Council of Australian Governments
Facial images	Facial images includes digital photographs, facial biometric templates or patterns, associated biographical information and other technical information related to those images (such as the time and date of capture and data capture standards used)
Holding agency	The agency that will receive and process requests from the Hub
Identification	A task where the biometric system searches a dataset for a reference matching a submitted biometric sample, and if found, returns a corresponding identity
IAA	Inter-agency agreements – agreement between participating agencies to authorise the sharing of biometric and biographic information via the Hub

[3] The glossary is available at http://www.biometrics.gov/referenceroom/introduction.aspx.

Term or Abbreviation	Meaning or expansion
IGA	Inter-governmental Agreement
IIS	Information Integrity Solutions Pty Ltd
LCCSC	Law Crime and Community Safety Council
Metadata	Information the Hub generates and retains about the transactions it processes, for example, the agency request reference and the time and date of the request. The metadata does not include the *content* of the transmitted request or response, that is it does not include the image itself or biographic or biometric information
NFBMC	National Facial Biometric Matching Capability Program
NISCG	National Identity Security Coordination Group
Participating agencies	Selected Commonwealth, State and Territory agencies undertaking law enforcement, national security and service delivery activities and authorised to use the Hub under the IGA and interagency agreements
PbD	Privacy by Design
Portal	A web based user interface to the Hub
Project	The Interoperability Hub project
Requesting Agency	The agency making the request for biometric or biographic information via the Hub
The Hub	The Interoperability Hub that is a central part of the NFBMC
The Privacy Act	The *Privacy Act 1988* (Cth)
TIC	Transport and Infrastructure Council
Unique Identifier	Letters, numbers, or symbols or a combination of these, such as driver licence or passport number or potentially a mobile phone number, which agencies use to identify, or verify the identity of an individual.
Verification	A task where the biometric system attempts to confirm an individuals' claimed identity by comparing a submitted sample to one or more previously enrolled templates

3. Overview of the NFBMC initiative and associated information flows

The NFBMC is a program of work being undertaken by AGD to maximise the potential for facial biometrics to prevent fraud, support law enforcement, promote national security and streamline service delivery, while maintaining robust privacy safeguards.

The project drivers include:

- The current reliance on manual ad hoc data sharing arrangements, which are unsuited for time critical matters and come with uncertain accountability
- Limited ability to detect individuals with multiple fraudulent identities (current searches are primarily name based)
- Inconsistent legislative restrictions on interagency data sharing
- Incompatible ICT systems
- Siloed driver licence image holdings with inconsistent facial recognition

The Capability will adopt a 'hub and spoke' technical architecture for the purposes of facilitating the transmission of identity-related requests and their respective responses, from select government agencies (participating agencies) via the Hub to other participating agencies. Participating agencies would include relevant Commonwealth agencies and (subject to agreement of state governments) state police and road agencies, which would access the Hub via coordinated national arrangements facilitated by CrimTrac and AustRoads respectively.

The key components of the NFBMC are:

- The Hub, which will facilitate the sharing of facial images between participating agencies, which can then match these images using their own facial recognition systems and return a response through the Hub
- A national driver licence facial recognition solution, which is currently under consideration, with AustRoads commissioning a business case for consideration by States and Territories, and which, if approved and developed, would support image sharing amongst road authorities and enable agencies connected to the Hub to match against these images
- A consistent legislative framework across all jurisdictions to enable the sharing and matching of facial images, while maintaining robust privacy protections
- Common technical standards for the capture and storage and transmission of facial images and related data and national training standards and competencies for personnel undertaking facial recognition and related functions
- Robust governance and accountability arrangements for ongoing monitoring and oversight of the NFBMC, including the conduct of independent PIAs.

The Hub will be managed by AGD and might at some point be provisioned on infrastructure set up by an outsourced service provider. AGD advises the Hub will be located in a secure facility, most likely in a central location; it would not be using cloud-based services. Overseas agencies would not be given access to the Hub at least initially – and any decision to expand access to overseas agencies would constitute a significant change in scope and must be approved through the NFBMC governance mechanisms.

3.1 Hub design – key features relevant to the PIA

This section describes features of the Hub that are most relevant to the analysis and assessment of privacy risks for the PIA. As will be discussed later in this report, some of these features limit risks, or support privacy protection. Others raise issues for consideration.

The description is not intended to be comprehensive. A comprehensive description of the Hub, to the extent it is developed and/or can be made available, is in the project documentation, including that reviewed for the PIA and listed at Appendix 1.

The features noted relate to the policy decisions taken that affect the Hub's design, its operation and technical capability.

3.1.1 Policy decisions affecting Hub design

IIS notes that the Hub design seeks to apply PbD and it has identified a number of policy decisions that are very consistent with this approach in the sense that they are privacy protective. These include that:

- The NFBMC has adopted a hub and spoke architecture
- The Hub will not store biometric or biographic content, although it does have the potential capacity (through reconfiguration or re-design) to do so
- The Hub will store some 'metadata' about each transaction it transmits but this information would be strictly limited
- The Hub will not have capacity to do any biometric analysis or matching
- The guiding principles for the Hub development include that:
    - The Hub has no role in identity resolution
        - The Hub is effectively neutral in that it will be up to the holding agencies to decide whether to respond to requests and how, and for requesting agencies to decide if there is a match
    - The participating agencies, as the data owners maintain access controls
    - The Hub will include robust security and will be subject to rigorous accountability.

The Hub facilitates two types of matching:

- Verification – which involves one-to-one matching of both biographic and biometric information
- Identification – which involves matching against images only, or with partial biographic information, in the context of law enforcement activities.

The risk that the match results will include false negatives or false positives increases very significantly for identification matching. AGD has been calibrating the Hub policy and design approach accordingly, for example, access and security arrangements are being designed to take account of the increasing risks associated with identification matching. Access to this more risky matching

category will be limited to a handful of expert users from each agency who are specialists in performing identity resolution.

The Hub design will provide the agency receiving requests to be assured of the purpose and authorisation in all transaction types (verification, identification and data sharing). In the case of verification used in the context of service delivery, it is expected that the individual concerned would be aware of and have consented to the match.

Implementation of the different functionality will be undertaken in a phased approach, starting first with the basic verification matching and data sharing transactions, then the identification services, which involve more complex information flows and arrangements, being rolled out in later phases.

The Hub is being designed to be highly scalable. It is expected to be able to accommodate significant expansion in the volume of images matched, the number and type of organisations connected to the Hub, and potentially the types of data beyond images that might be transmitted. It is also possible that in the future the Hub could be available to private sector organisations, for example, where those organisations have a legal obligation to be satisfied about a person's identity, such as in the context of anti-money laundering and counter terrorism financing.

3.1.2 Hub technical features

The Hub is not a centralised database for facial images. Its function is simply to receive data (in the first place, facial images and/or limited biographic details), transform it into a format acceptable to the holding or receiving agency and deliver it to that agency. The Hub in isolation will not store any biometric or biographic information (although the information collected in audit logs could act as a 'pointer' to such information held by participating agencies).

Participating agencies will access the Hub via a portal, which is a web based user interface, or via a system-to-system interface.

A major rationale for the hub and spoke approach is to shield agencies from changes in biometric software and the underlying ICT systems in the context of information exchange – the Hub will be a service orientated architecture that accommodates for/addresses the fact that agencies use different facial recognition software and engines and these will likely change over time.

3.2 Brief description of Hub functions and associated information flows

AGD has identified five key functions that the Hub will be designed to support, which by their nature will have varying impacts on privacy. Some details are still to be finalised but in broad terms the functions are:

- Image retrieval (search of agency databases using biographic information or unique identifiers to retrieve existing images held on an agency's database)
- Image-based verification (one-to-one comparisons of a captured image with a specific image held on an agency's database)

- Image-based identification (one-to-many comparisons of a captured image against all the images held on an agency's database; one-to-few comparisons of a captured image against segments of images held on an agency's database)
- Incremental updates of shared image galleries
- Occasional bulk data transfers.

The table below gives an indication of the information flows associated with each function. The information captured by the Hub in audit logs as it performs its role is described separately below and is not included in the table.

Function	Use cases	Participating agency – making request	Participating agency – providing response
Image-based verification (one-to-one)	Agency has an individual's image and biographic information and seeks to verify their identity	Submits image and biographic information and purpose/justification, which in the context of service provision would include individual notice and consent	Undertakes search provides match/no match response
Image search/retrieval (one-to-one or one-to-few)	Agency has biographic details but no image	Submits biographic data or a unique identifier, and purpose/justification	Undertakes search according to agreed rules and provides facial image (or images) and associated identity information or no match found
Image-based identification (one-to-few, one-to-many)	Agency has images but limited or no associated biographic information	Submits a facial image or image with associated demographic information, match threshold and purpose/justification Once data is received a human operator will need to make a determination about which result is the subject	Undertakes search according to agreed rules and provides match score, a set or subset (depending agency rules) of possible matching facial images and associated identity information or no match found
Incremental updates of shared image galleries	Agencies provide images and biographic information for target or watch lists	Submits images and biographic information	Advises request received Adds information to target or watch lists
Bulk data transfers (occasional)	Agency has a batch of cases and wishes to determine which include legitimate identities	Submits batch of data (images and related information)	Confirms request received Undertakes search according to agreed rules Once all matches undertaken, provides a batch of sets or subsets (depending agency rules) of possible matching facial images and associated identity information

3.2.1 Metadata generated in the context of the Hub's operation

The Hub sits between the participating agencies and for each request and response will:

- Authenticate the agency user and confirm their authorisation to use the Hub

- Validate the request
- Transform it in accordance with business rules and interagency agreements
- Route the request
- Receive confirmation that the request was received and transmit the response to the requesting agency.

The Hub does not retain any record of the biometric or biographic content of a request or response but it does generate metadata for audit and performance testing and reporting. The full details of the metadata are still being decided but are likely to include:

- User or system that initiated the request
- Authentication and authorisation outcome
- Request type
- Target data
- Service priority
- Holding agencies to which the request is directed
- Agency request reference or transaction number
- Timing data.

AGD is considering if the Hub should also retain the MD5 message-digest algorithm or cryptographic hash for each image with the intention of further facilitating participating agencies audit or investigation activities.

3.3 Current and proposed NFBMC governance arrangements

There are a number of current and proposed governance arrangements for the Hub project and the wider NFBMC. The key features of the proposed arrangements relevant to this PIA include:

- The AGD Project Board for the National Facial Biometric Matching Capability (Project Board)
    - The project board, which has the authority and responsibility for the project, is chaired by the Senior Responsible Officer, and includes the Chief Information Officer, the Chief Financial Officer and representatives from the IT Division, Identity Security Policy Section and the Document Verification Service Team.
- An interagency programme steering committee to oversight the implementation of the NFBMC
- An appropriate body, such as the National Identity Security Coordination Group (NISCG) with responsibility for ongoing monitoring and oversight of the NFBMC at the national level
- Reporting by the NISCG to the Council of Australian Governments (COAG) Law, Crime and Community Safety Council (LCCSC), which includes Attorneys-General and Police Commissioners that have portfolio responsibility for privacy in most, if not all jurisdictions

and which would exercise ministerial oversight of the NFBMC and which would be responsible for its establishment and operation and which would need to endorse any significant policy changes

- An inter-governmental agreement (IGA) to be developed to outline the purpose and scope of the information sharing between the Commonwealth, states and territories via the NFBMC
- Inter-agency agreements (IAAs) to be developed between participating agencies to authorise the sharing of biometric and biographic information via the Hub, dealing with matters such as permitted uses and disclosures and facial recognition matching thresholds.

4. Privacy regulator consultations

AGD asked IIS to consult the Australian Privacy Commissioner, and Privacy Commissioners or a nominated representative for each of the States or Territories, as part of its information gathering for this PIA. IIS understands that AGD anticipates separately consulting the Commissioners about other aspects of the NFBMC. The Commissioners also anticipate being consulted and providing advice within their own jurisdictions.

The list of Commissioners consulted is at Appendix 1.

The consultations involved an AGD presentation on the NFBMC, including the proposed Hub functionality, followed by round table discussions. They identified a range of potential risks related to:

- The Hub design, operation and governance
- State and Territory agencies' use of facial biometrics in the context of the Hub
- The potential overall impact of the NFBMC once rolled out
- The potential future development of the NFBMC.

Points 2, 3 and 4 are outside the scope of this PIA and IIS understands they would be considered in future PIAs at Commonwealth or State and Territory levels. IIS' discussion and recommendations do not address these risks other than to identify the need for governance processes to address significant changes to the NFBMC.

IIS's PIA takes account of the matters the Commissioners raised but the views expressed in this report are its own and are not intended to represent the views of the Commissioners.

The risks raised in the discussion are listed below and where relevant are reflected in more detail in the discussion on privacy risks in Section 6 below.

Hub Design

- Security risks including the potential for the Hub to be hacked and the reliability and probity of agency users
- Mechanisms to provide assurance to the holding agency of the reason for and legitimacy of a request via the Hub

- The nature of Hub audit and logging data and the potential for individual surveillance or tracking.

Hub operation and governance

- The governance and accountability arrangements which are considered to be central to the safe operation of the NFBMC and AGD's accountability for the system if things go wrong
- Transparency of both the hub project and its subsequent deployment and growth in deployment, including if and when this PIA report might be published
- Ensuring the Hub design and operation is informed by a keen awareness of community values about the use of their personal information; this is particularly important in the context/climate of recent national security initiatives (e.g. data retention)
- Resources available, including for the accountability bodies, to provide for effective oversight of the system
- The ability of accountability bodies (including privacy commissioners and ombudsman) to conduct end-to-end audits or investigations where issues are cross jurisdictional
- Possible involvement of anti-corruption bodies in oversight or investigations
- The extent to which AGD has responsibility for (or should have responsibility for) the Hub and for what goes on at the participating agencies
- Oversight and audit of AGD as the Hub manager.

State/Territory Hub participation

- The nature of the consent for verification matching in the context of service provision including:
  - Whether additional levels of consent are required
  - Whether individuals actually have real choice or whether it is more appropriate to recognise that compulsion is involved (or at best, very little real choice) and to ensure that accountability and incident handling arrangements are designed accordingly
- Impact on individuals' right to request to see a trail of the use of their personal information and need to maintain a record of any disclosure of personal information. Consistent compensatory legislative safeguards may be required.
- The issue of the shifting quality of data held by agencies, as well as the current flaws of the Document Verification Service (i.e. is the current data set considered to be the 'true' data set)
- The fallibilities or accuracy shortcomings of facial biometric matching technology (including the false positive and false negative rates)
- Responsibility/channels if things go wrong for individuals

- The compliance costs to each participating agency and oversight agency, including the increase in resources needed for privacy regulators or ombudsman, police or service delivery agencies.

Overall impact of the NFBMC now and into future

- The scope of NFBMC, which seems very broad and which, with the inclusion of service delivery, seems to anticipate facial biometrics being used in the context of almost all government activities
- Whether the design, development and implementation of the Hub is a proportionate response to the scale of identity crime prevention, counter-terrorism, law enforcement and service deliver objectives:
    - What proportion of these problems the NFBMC will address
    - Is this measurable – accurate, measureable statistics/projections of benefits will be required to illustrate the necessity of the Hub
- The relationship between the NFBMC and other government identity/biometrics projects, such as the work being undertaken by the Digital Transformation Office around a trusted digital identity policy and the CrimTrac Biometric Identification Services project
- Whether the proposed efficiencies of the Hub will erode over time, as criminals adapt to the new model/advances in technology
- Potential for privacy benefits, for example in assisting citizens to recover from identity crime
- Consideration of legislatively based limits and strengthened governance arrangements on the use of the Hub, for example, expanding to other types of biometrics.

5. NFBMC benefits including privacy benefits

This PIA is being undertaken on basis that the Government has already taken the decision that the facilitated exchange of biometric images will help prevent fraud, support law enforcement, promote national security and streamline service delivery and that this is best undertaken by the development of an exchange Hub. It is outside the scope of the PIA to address this decision.

IIS has taken account of the potential NFBMC benefits, summarised in this section, in undertaking its risk assessment. IIS notes that PIAs proposed as part of the further development of the NFBMC, including those by States and Territories, might consider whether facial biometric matching via the Hub is proportionate to the risks in question.

The NFBMC design started with a conscious decision to consider privacy impacts. The Hub Concept of Operations notes that the decision to adopt a Hub and spoke architecture included that this model would ‘minimise privacy impacts when compared to other potential models’.

The project documentation reviewed for the PIA has identified a range of potential benefits of the implementation of the NFBMC of which the Hub is an integral part. These include:

- Enhanced national security

- Better law enforcement
- Strengthened border management
- Improved fraud prevention
- More trusted ID credentials
- Accountable information sharing
- Better road safety
- Improved background checks
- Economies of scale, and
- Streamlined service delivery.

In discussions with AGD staff and the Privacy Commissioners these benefits were explored further and there was discussion, for example, of the utility of the Hub to assist agencies in locating missing persons or investigating and prosecuting child sex offenders.

Some of the identified benefits relate directly to improved privacy protection. In particular, in the light of increasing number of Australian's who fall victim to identity crime each year, the discussion with Privacy Commissioners identified the potential for assisting individuals to recover from identify fraud or theft; this is currently notoriously difficult to measure.[4]

Other benefits included potential for improvements in data quality, for example, sharing with other agencies, with individuals' consent, inaccurate information identified in the context of a matching activity.

6. Findings on risks and recommendations

6.1 Approach to the risk assessment

6.1.1 General factors affecting risk assessment

As specified in the scope for the PIA, the focus of this analysis is the central Hub and a high-level consideration of the governance arrangements for its operation within the context of the NFBMC. The scope does not extend to the other components of the NFBMC, including the proposed National driver licence facial recognition solution, or to the collection, use and disclosure of personal information at the agency interfaces.

This section considers the potential impact of the NFBMC and the Hub broadly to provide context for the discussion below, particularly in relation to governance arrangements.

[4] The scale of identity fraud in Australia is explored in AGD's 2014 report *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot* which is available at http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Trends-in-Identity-Crime.aspx

Central to the analysis is the fact that biometric information is considered intrinsically sensitive and is treated so in the Privacy Act.[5] Amongst other things, it is information that can uniquely identify a person. IIS has also taken into account the significantly different risks that arise in the context of 'identification' as opposed to 'verification' matching processes; in the former case, which involves one to many matching, there is greater potential for errors to occur.

IIS considers there is potential for the implementation of the Hub to have an impact on the circumstances in which facial biometric information is shared, by whom and the volume of images shared. This is relevant to the governance of the Hub initially and if and how its use expands beyond the initial implementation. Significant growth in use of the hub could affect privacy risks both at the individual agency level and at the level of the system as a whole. In IIS' view the privacy impacts of the whole system could well be greater than the risks at individual agency or Hub level.

IIS also notes that the NFBMC is intended as a multi-jurisdictional activity and responsibility for the Hub will fall to Ministerial and senior officer level groups under the Australian governmental cooperative arrangements. While AGD is assisting with the development of governance arrangements, it will not have full control over how they operate in practice.

6.1.2 The application of the Privacy Act and APPs to the Hub

The starting point for any PIA is the requirements of the relevant privacy law, in this case the Privacy Act and the APPs. The APPs set the framework for the collection and handling of personal information including requirements in relation to security, use and disclosure. The APPs also give individuals rights to seek access to their personal information and to seek to have it corrected.

AGD as a Commonwealth agency is subject to the Privacy Act, including in its role as the Hub manager. However, its obligations under the Act in the context of the Hub will depend on whether it is considered to collect or hold personal information.

Personal information is defined in the Privacy Act as

> information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.[6]

In providing guidance on the scope of concept of personal information, and in particular on when information might be about an individual who is 'reasonably identifiable', the Office of the Australian Information Commissioner advises that this depends on matters such as:

- Other information either held by or available to the APP entity that holds the information

[5] Privacy Act, s.6(1) definition of sensitive information
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html

[6] Definition of personal information – ibid.

- Whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'.[7]

As noted in the earlier sections of this report, the Hub has been specifically designed to be a neutral transmitter of information and to retain a very limited set of information about the transactions it processes (see Section 3.1.1 and Section 3.2.1 above).

The information transferred through the Hub will contain biometric and/or biographic information including name and date of birth, or unique identifiers. IIS considers that it is at least arguable that the Hub, in its momentary handling of this information as it transforms it into appropriate formats for the participating agencies, is handling personal information.

The information, or metadata, the Hub generates for each transaction is, as noted, deliberately limited. IIS is satisfied that the metadata the Hub holds would not, on its own, be sufficient to identify the subject of a request.

IIS notes that this assessment is based on its understanding of the Hub's current configuration. Although not currently intended, IIS understand that it would be technically feasible to change the nature and extent of information the Hub holds. Were such a change to be contemplated, IIS considers that appropriate governance mechanisms are required to address the implications of such a change including on privacy, including but not limited to a further privacy impact assessment.

While metadata in the hands of the Hub might not identify individuals, IIS understands that it could act as a 'pointer' that could be used by the requesting or holding agency, in conjunction with their own systems to establish the circumstances of the request, including which officers were involved and which individual or information was in question. IIS also understands that AGD could similarly seek to gather and join up information 'available' from participating agencies. However, given the Hub's currently intended role and operation, IIS understands it would be unlikely to have any reason or need attempt this.

While it might be possible to argue the case, IIS considers that it is unclear at this point whether the Hub would collect personal information. Possibly a strict legal argument might conclude that it does not.

Nevertheless, IIS considers there is considerable value in AGD choosing to commit to complying with the APPs in its role as Hub manager, because:

- It would be consistent with AGD's commitment, for example in the NFBMC Blueprint, to 'maintaining robust privacy safeguards'

[7] Guidelines to the Australian Privacy Principles, Chapter 8, B86-B96 http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-b-key-concepts#personal-information

- Conversely, it might be harder for AGD to demonstrate its commitment to privacy if it takes the view that the APPs do not apply to the Hub
- Application of the APPs would provide a structured framework to assist AGD to identify and manage privacy risks in the context of the Hub, and the NFBMC
- Interpretations of definitions of personal information are tending to become broader in response, for example, to rapidly improving Big Data analytics, the rapid expansion in the creation, exchange and collection of metadata and other computing and technology changes.[8] Even if the Hub is not considered to be collecting personal information now, this view might well change in the future.

1. APPs to apply to information the Hub collects, transmits or holds

IIS recommends that AGD in its role as Hub manager commit to complying with the APPs, whether or not the Hub is legally considered to collect or hold personal information.

6.1.3 Structure of findings and recommendations

In this section on its findings and recommendations, IIS discusses the potential privacy risks it has identified to date in the Hub design and its proposed operation and governance.

In line with recommendation 1 above, IIS has worked on the assumption that the APPs would apply. In this context IIS considered whether the Hub design raises any risks as far as compliance with the APPs. Similarly, IIS considered if the Hub's proposed operation and governance raises APP compliance risks. The table Appendix 2 considers the possible risks against the APPs. The key APP risks identified are discussed below.

IIS has also considered if there are risks arising in the context of any broader privacy concerns for this type of project and taking account of privacy best practice. The risks identified following this analysis are also discussed below.

6.1.4 Overall view on privacy risks within scope of PIA

IIS considers that AGD's approach to the Hub design process has been generally consistent with the requirements of the APPs and good privacy practice. It has not identified any significant risks in the Hub design. IIS has identified areas where it considers some extra steps are needed to maintain the focus on privacy and good privacy practice. These include:

- The ongoing management of privacy in the Hub design
- The metadata the Hub generates about the transactions it handles
- The Hub access and security arrangements.

[8] See for example, the Privacy Commissioner's decision in relation to an individual's request for access to metadata about them to Telstra at http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-determinations/2015-aicmr-35

IIS also considers that AGD's approach to the Hub's operation and the likely governance arrangements is also consistent with the APPs and it has not identified any significant compliance risks. However, it has made a number of recommendations to strengthen privacy practices. These recommendations take account of the multi-jurisdictional nature of the NFBMC and aim to promote continued privacy good practice to help ensure the aspiration of 'robust privacy safeguards' is delivered. The areas in which IIS considers there are potential privacy risks include:

- The scope of the NFBMC
- The privacy management framework
- The extent to which the development and operation of the Hub are conducted openly and transparently
- The NFBMC governance arrangements including the governance of change.

6.2 Findings and recommendations – design of the Hub

6.2.1 Implementing privacy compliance and good practice

APP 1.2 requires agencies to take steps that are reasonable in the circumstances to implement practices, procedures and systems to ensure they comply with the APPs. In this regard IIS commends AGD's adoption of PbD as a guiding principle for the Hub design and implementation.

The assessment IIS has undertaken on the project design to date indicates that this has been a useful framework for minimising privacy risks. Approaches consistent with PbD include the Hub and spoke architecture l (as opposed to a central data base), data collection limitation and strong security.

IIS considers that in continuing this approach it will be important that the Hub design takes into account the Hub's future use in terms of volume, number and nature of participating organisations and nature of information exchanged. IIS also considers that broad thinking, rather than a mere compliance approach, about privacy risks, should inform the design work. This would mean, for example, bearing in mind risks to individuals as well as to agencies, and considering risks such as the potential for function creep.

2. Hub design informed by a broad view of privacy and the potential overall impact of the NFBMC

   (a) IIS recommends that AGD ensure that its further development of the Hub, and the governance arrangements for the operations of the Hub, reflect a broad view of the concept of privacy, as opposed to a strict legal compliance view.

   (b) IIS recommends that the Hub design and governance arrangements should, from the outset, take into account the Hub's likely future use, both in terms of the number and nature of participating organisations, as well as the volume and nature of information exchanged and the potential impacts on privacy.

6.2.2 Collection of Information

APP 3.1 requires agencies to limit the collection of personal information to that which is necessary for, or directly related to, their functions and activities.

A factor that will affect the privacy impact of the Hub is the metadata that it generates. Of necessity, the Hub will generate metadata in order to manage its processes. In addition, IIS understands AGD would have obligations under the Protective Security Policy Framework to keep audit logs. IIS also understands that Hub metadata could assist participating agencies to meet their responsibility to ensure their access to the Hub is authorised and appropriate. It could, for example, provide data for audits or investigations or provide alerts where an agency user's pattern of use appears suspicious or if there appeared to be external attempts to 'hack' Hub infrastructure.

However, metadata trails can also carry privacy risks including the potential to support increased tracking or surveillance of individuals. The metadata the Hub is expected to collect is listed in Section 3.2.1 above. IIS considers that, on its own, the information does not include personal information. It considers, from its review of the material provided, and its discussions with AGD, that the risk that metadata generated by the Hub itself will facilitate greater tracking or surveillance of the everyday activities of individuals is low. There might still be a risk that the Hub will nevertheless be perceived as leading to tracking and surveillance. IIS addresses this risk in Section 6.3.2. Here IIS considers that minimising the extent of metadata generated, as AGD is planning, is an important plank in minimising the risk of tracking and surveillance. The time for which metadata is retained will also affect privacy risks. This risk is discussed in below in the context of the APP security requirements.

6.2.2.1 Retention of metadata

Although IIS considers the potential for the Hub metadata to facilitate surveillance or tracking of individuals to be low, the risk will remain while data is retained. IIS considers metadata should be retained for the minimum possible and it suggests that there might be useful experience available from the Document Verification Service.

3. Limit metadata to that needed for operational purposes and agency audits or investigations

   (a) IIS recommends that AGD ensure the metadata generated by the Hub is the minimum needed to:

      (i) Effectively manage the Hub

      (ii) Provide assurance that access to the Hub is for legitimate and appropriate purposes

      (iii) Ensure participating agencies can monitor their access to the Hub and undertake investigations of possible nefarious staff activities.

   (b) IIS recommends that the nature of metadata generated, and the period for which metadata will be retained be transparent to citizens.

   (c) IIS recommends that metadata generated by the Hub be retained for the minimum period needed to support the purposes for which it is generated.

6.2.3 Dealing with Information

APP 6 requires organisations to limit the use or disclosure of personal information only to the purposes for which it was obtained or for related purposes, for a 'permitted general situation', or in

accordance with a range of other permitted exceptions including that the individual would reasonably expect or has consented or the use or disclosure is authorised by law.[9]

To the extent that the information the Hub collects, transforms and transmits is personal information, IIS considers that this use and disclosure is likely to be for the purpose for which it was obtained and therefore consistent with APP 6.

The Hub does not have a direct role in participating agencies' decisions about whether to release images or biographic information. The discretion remains with the holding agency. The Hub is being designed to provide some information about the purpose/justification for the request to support agency decision-making. IIS understands the purpose/justification could include information such as the seniority of the person making the request, relevant legal provisions authorising the disclosures or details to satisfy the holding agency that a disclosure of information would be consistent with the applicable privacy law in its jurisdiction.

IIS strongly supports this approach. It considers that the Hub design should provide for sufficient detail to allow for informed decisions about disclosure and to allow for effective auditing of the receiving agency's authority to make the request.

4. Records of authority to release information

IIS recommends that AGD ensure the Hub design supports agencies' ability to make well-informed decisions to release images or biographic data based on a clear understanding of the purpose and authority for the request.

6.2.4 Security

APP 11 requires agencies to take such steps as are reasonable in the circumstances to protect personal information from:

- Misuse, interference and loss
- Unauthorised access, modification or disclosure.

Agencies must also destroy or de-identify information when it is no longer needed for specified purposes.

'Best practice security' is identified as a design principle for the Hub. Clearly this is critical not only for protecting the privacy of individuals but also in ensuring the system can be trusted by participating agencies and the community.

The initial design includes a range of security features that indicate considerable work has been done on effective security approaches and IIS notes that the Hub project team will be focussing on testing and refining its security approach in its next steps.

[9] For permitted general situations see s.16B of the Privacy Act at http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s16a.html

IIS does not intend to comment in detail on security issues in light of the attention it is given in other forums, however a few issues emerged in its review of the background material. IIS also notes that security issues were a strong area of concern in the discussions with privacy commissioners. Issues identified so far are as follows:

- The fact that biometric and biographic information will be passing through the Hub for processing and transformation means there a vulnerability to security risks such as hacking and man-in-the-middle attack[10]
- IIS understands that information could remain in an agency's cache when it leaves a session unless the agency take steps to clear the cache
    - AGD advised in this regard that the way the Hub is rendering images should result in the browser not being able to cache them. It also noted that cache management occurs via agency/user specific settings. If needed, AGD would address this issue at a policy level
- Management of agency access to the system could also be an issue
    - IIS notes that in response to this security risk, AGD is proposing to disable and require re-authorisation of all user accounts at regular short, for example three monthly, intervals
- Experience with inappropriate police service access to sensitive data bases suggests this is an issue that could occur in the context of Hub access
    - IIS considers that high quality training and appropriate auditing and provision of assurance to the holding agency should be part of interagency agreements
- The potential for the capture and further use of images or biographic data returned following a request beyond what is expected by the nature of the request and surrounding processes.
    - While technical limitations can be implemented to restrict an agency's ability to save a response, there remains some risk that, for example, users will take screen shots or use a mobile phone camera to capture an image. IIS acknowledges that such actions might be breaches of the Privacy Act, employment conditions and/or the Crimes Act but also notes that such actions are difficult to control completely.

      AGD advised that consideration had been given to including an identification number across the face of the image but this idea had been discarded because it interfered with the efficacy of biometric matching and could increase the handling time of an image at the Hub thereby increasing security risks. Depending on how such an approach was implemented, this type of measure could also require the

[10] Wikipedia describes a man-in-the-middle attack as one where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Hub to interact with the biometric content of the messages, which is contrary to the design principles.

AGD noted that agencies could include a stamp on an image. IIS considers this is an issue worth pursuing. While out of scope for this PIA, IIS has noted it as an issue to consider in the future development of the NFBMC.

5. Strengthening of some security measures

   (a) IIS supports the access management approach proposed by AGD and recommends disabling and re-authorising all users and their level of authority at regular short, for example, three monthly intervals.

   (b) IIS supports the Hub project emphasis on training and standards and recommends that AGD ensure these address:

      (i) Appropriate personnel access to and use of the Hub

      (ii) Policy and procedures on the issue of image caching by agencies' online systems.

   (c) IIS recommends that AGD, in developing interagency templates, ensure they

      (i) Include strong controls for ensuring that only authorised individuals, cleared to Protected or higher as needed, can gain access to the system and only be authorised to undertake activity that reflects their level of authorisation

      (ii) Require auditing of such access and provision of assurance about the appropriateness of access to biographic or biometric data to the holding agency.

In recognition of the very significant potential risks and potential intrusions that arise in the context of one-to-many matching to identify individuals, IIS strongly supports the approach in the Hub System Access Flows that this particular functionality be tightly controlled; it would only be available to a select number of expert users within law enforcement agencies or specialist fraud investigators, and that service delivery agencies would not have this access. The Privacy Commissioner meetings expressed similar sentiments.

6. Access to the Hub to identify individuals to be strictly controlled

   (a) IIS supports the approach proposed by AGD and recommends that access to one-to-many matching be tightly controlled and limited to a few law enforcement agency uses (service delivery agencies should not have this access).

   (b) IIS also supports AGD's general approach of limiting and controlling access to the Hub based on assessed risks in matching processes.

6.3 Findings and recommendations – operation/governance of the Hub within the current scope of the NFBMC

6.3.1 Proactive privacy management

APP 1.2 (policies, procedures and systems to ensure compliance with the APPs) is also relevant to AGD's operation of the Hub. There will be a range of policy issues to consider as the Hub moves from design to implementation. These issues could include developing relevant policies and procedures, finalising and implementing security measures, including those identified in the IIS recommendation above, and managing any involvement of third parties in the provision of the Hub's services. As the Hub becomes operational there are also likely to be new issues to consider. For example, law enforcement or national security bodies authorised to obtain information overtly or covertly might be interested in the information flows through the Hub and AGD should have policy and processes to deal with any such requests.

IIS has also noticed a tendency, for example, in the draft governance arrangements to convey that privacy is dealt with by compliance with privacy laws, rather than as an issue that needs broader consideration. As recognised in the OAIC *Guide to Undertaking Privacy Impact Assessments*, in reality, and particularly in the design and implementation phases of a project, such a narrow focus can lead to an under identification of privacy risks and impacts.

Without a systematic focus, there is a risk that AGD will consider privacy issues have been dealt with once the Hub design is complete and that the focus on privacy will dissipate. IIS considers that dealing with issues such as those noted above in the context of an overall privacy governance framework would ensure a continued focus on PbD and good privacy practice as well as promoting compliance with the APPs.

7. Proactive privacy management

IIS recommends that AGD ensure that it has in place a privacy governance framework both to manage the Hub as it moves to BAU and when it is fully incorporated into BAU, which takes a broad view of privacy and commits to privacy best practice.

IIS notes that AGD is proposing, in the context of assessing the overall benefits the NFBMC provides, to ask agencies to quantify the benefits they expect to achieve through its use and to monitor and report on the achievement of those benefits over time. To assist with this process, AGD will work with agencies to develop a consistent methodology for identifying and costing benefits.

IIS strongly supports this activity. Its concern from a privacy perspective is that where costs are being assessed they should include all costs, including cost of governance such as compliance costs, resources likely to be consumed by regulators and other oversight bodies, audit, assistance to individuals and the community and complaint handling.

8. Benefits assessment to take account of privacy governance costs

(a) IIS recommends that in developing the methodology for identifying and costing benefits AGD and participating agencies should also bring into account all costs involved, including costs of privacy governance, such as:

(i) Participating agency compliance, and regular monitoring and audit costs

(ii) Resourcing of privacy regulators and other oversight bodies

(iii) Assistance to individuals and the community and complaint handling

6.3.2 Open and transparent management of personal information

APP 1.1 set out as an objective that agencies manage personal information in an open and transparent manner. APP 1.3 requires agencies to have a clearly expressed and up-to-date privacy policy setting out matters such as the nature of personal information collected and held for what purposes and how it is handled.

IIS considers that for a project such as the NFBMC, transparency at the individual and system level will be a key element of good privacy governance. The Privacy Commissioner meetings had a similar concern for transparency, particularly in relation to this PIA report, which they considered should be circulated to them and published.

IIS also considers that, in light of the experience of a range of major projects at all levels of government affecting the handling of personal information, in the absence of strong public engagement, there is potential for the perception that the Hub will facilitate increased tracking and surveillance to take hold.

IIS considers that the best defence here is:

- A strong effort to engage the community
- To make the development and implementation process as transparent as possible
- Demonstrate that strong governance, accountability and redress mechanisms will be developed, implemented and well funded

IIS also notes that adequate transparency will require more than simply making material available via a website. This is important; community trust in a project such as the NFBMC and the Hub is likely to benefit from real public engagement. Experience shows there is potential for strong adverse reaction if transparency processes are not well managed.

9. Project to be conducted transparently

(a) IIS recommends that AGD ensure that as soon as possible, and to the extent possible, information about the NFBMC and the Hub is in the public domain.

(b) IIS recognises AGD's intention to circulate and publish this PIA and recommends that it be published as soon as practicable.

(c) IIS recommends that AGD design and implement a proactive and transparent community engagement approach to support the introduction of the Hub.

IIS understands that IGAs are available on the COAG website; and that the Office of the Australian Information Commissioner's Information Publication Scheme promotes the public availability of such agreements. IIS considers that an additional measure once the NFBMC is operational would be to establish a publicly available register of the IAAs as they are developed.

10. Transparency in Hub use and intergovernmental agreements

(a) IIS recommends that all of the interagency agreements between participating agencies authorising information sharing via the Hub should be included in a register.

(b) IIS also recommends that the register be available for public inspection or that the interagency agreements are otherwise published and that all this documentation be easily available from the one source.

6.3.3 NFBMC Scope

The NFBMC Blueprint provides that its vision is to 'maximise the potential of facial biometrics to prevent fraud, support law enforcement, promote, national security and streamline service delivery, while maintaining robust privacy safeguards'.

IIS's initial reaction was that the inclusion of streamlined service delivery in the vision provided for an almost unlimited scope for the NFBMC. Amongst other consequences, such a broad scope would make it very difficult to understand the full longer-term privacy implications. The Privacy Commissioner meetings highlighted a similar concern. The commissioners also identified an additional complication arising from the potential, but as yet unclear, relationships between the work on digital identities being undertaken by the Digital Transformation Office and similar initiatives being undertaken by other agencies including CrimTrac.

IIS understands that the vision for the NFBMC is intentionally broad and that the Hub, within its design limitations, could well expand in ways not currently specified, including allowing use, of certain functions, by private sector organisations. However, IIS also understands that the initial focus is intended to be much tighter and, in particular, the service delivery element is limited to use by initial participating agencies for the purposes of facial biometric matching in the context of providing their own services.

11.NFBMC scope

IIS recommends that AGD's documents and communications in relation to the NFBMC, including design specifications, undertakings and governance proposals, make clear the limits on the initial scope of the NFBMC. It must be made clear that if any change occurs in either the number or type of participating agencies, in the nature of the biometric and/or biographic information transmitted, or the information held in the Hub, this would constitute a move beyond the initial scope and therefore trigger further privacy assessments.

6.3.4 NFBMC Governance arrangements

Section 3.3 above sets out the proposed governance arrangements for the NFBMC, including the various bodies to be involved and their roles.

IIS considers that the governance arrangements for the Hub in the context of the NFBMC will be a critical factor in ensuring privacy issues are given appropriate consideration in the final design and implementation of the Hub, as it transitions to 'business as usual' and in ensuring privacy safeguards are in place and working.

Governance of the Hub was also a matter for considerable discussion in the Privacy Commissioner meetings. A major theme in the discussions was the general ineffectiveness of IGAs in providing strong governance where there were multiple stakeholders and where decision-making, accountability and responsibility are shared amongst the stakeholders rather than resting with one person/body. In such circumstances where roles and responsibilities are not clearly articulated, it is difficult to make decisions and attendance and interest tend to degrade over time.

IIS does consider there is a risk that under the proposed arrangements accountability and governance could be so dispersed that it becomes 'accountable to all equals accountable to none'.

The Privacy Commissioner meeting canvassed a range of options, including the possibility of establishing a separate incorporated body to manage the Hub. However, it was recognised that such arrangements would be difficult to promote in the current fiscal environment.

The meeting also noted some examples of what seem to be more effective governance arrangements; for example the arrangements for the personally controlled electronic health record (PCEHR) were noted as moving in a positive direction and could provide a model for the Hub governance. The forthcoming changes to the PCEHR respond to a range of identified difficulties in the current governance arrangements including:

- Lack of transparency in decision-making processes
- Ineffective consultation with stakeholders
- Inefficiencies and lack of coordination in governance arrangements.

The new arrangements include the establishment of a statutory authority to manage the PCEHR. The authority would have an independent board that would be supported by a series of committees including a Consumer Advisory Committee and a Privacy and Security Committee.[11]

IIS shares the experiences and concerns mentioned in the Privacy Commissioner discussions. However, it appreciates that it could be difficult to get governance perfect, including as it affects privacy, from the outset. It could be a matter of trying and testing options. IIS considers there is a range of issues that should be addressed in the initial arrangements, including the IGA (and again in periodic – at least three yearly – systematic reviews of the system).

A question that was raised in discussions with Privacy Commissioners but not fully resolved was the options to provide independent privacy advocacy into the governance arrangements. The current arrangements do include some privacy interests. As noted at Section 3.3 above, the Commonwealth, State and Territory Attorneys-General are on the LCCSC and for the most part have privacy responsibilities within their portfolios. The Australian Privacy Commissioner also participates on the NISCG, an officials-level body that supports the LCCSC, but prefers to take observer status in the interests of retaining independence in fulfilling his regulatory oversight functions.

IIS recognises that it is difficult to find the right person or institution independent of law enforcement or national security that is able to offer perspective of everyday people. The United States Privacy and Civil Liberties Oversight board provides an interesting model, and its composition could offer suggestions for the type of people that might be relevant for the NFBMC.[12] In Australia, the person might come from academia or from one of the ethics centres.

12. The people's voice in governance arrangements

IIS recommends that the membership of governance bodies with a role in monitoring the operations of the NFBMC or in making decisions about changes in its scope or operations include an independent representative able to present individuals' perspectives.

IIS considers that the compliance regime for the Hub, including audit and complaints management, should be properly resourced throughout the system. It suggests that, consistent with financial information governance principles each participating agency, and the Hub, should be required to meet the costs of its own independent assurances in regard to privacy as a condition of participation, including independent PIAs (as AGD already contemplates) and subsequent audit and other continuing accountability measures.

IIS also considers it critical that external oversight of the Hub in the context of its role in the NFBMC is commensurate with data flows; the more information sharing the more oversight needed. A critical

[11] The report of the PCEHR review leading to these changes is available at http://health.gov.au/internet/main/publishing.nsf/Content/17BF043A41D470A9CA257E13000C9322/$File/FINAL-Review-of-PCEHR-December-2013.pdf

[12] See https://www.pclob.gov

factor here will be to ensure that inter-jurisdictional cooperation between government regulators (Privacy Commissioners, Ombudsman etc) is facilitated and is commensurate with the extent of data exchange anticipated under the IGA.

IIS considers that, and this was strongly confirmed in Privacy Commissioner meetings, it is also critical to ensure regulators are sufficiently resourced, and are given additional resources if required, to effectively oversight the NFBMC arrangements.

13. Matters to be addressed in high-level intergovernmental agreement covering the NFBMC

(a) IIS recommends that the inter-governmental agreement that will set the framework for cross-jurisdictional sharing of biometric data via the Hub should:

(i) Ensure that privacy interests are appropriately represented on the body tasked with being accountable for the delivery and management of the Capability.

(ii) Require the receiving agencies to resource compliance audits by both themselves and the holding party or pay for independent audits to provide assurance to data holders

(iii) Require holding and receiving agencies to retain information that facilitates audits of the use of the Hub and regular systemic reviews of the system

(iv) Ensure resourcing for external oversight of the Hub by privacy regulators, Ombudsmen or anti-corruption bodies is commensurate with data flows and that there are no impediments to cooperation and information sharing between oversight bodies where information is shared between jurisdictions

(v) Require participating agencies to have in place well-resourced 'safety net' mechanisms to effectively support individuals who may be adversely affected by agencies' use of the Hub and to respond efficiently and respectfully to any complaints.

Key guiding principles for the NFBMC include that participating agencies remain responsible for their information, and for decisions about whether a request is verified, whether to release biometric images, and whether there is a match. As noted at Section 3.3 the arrangement between agencies, including matching accuracy thresholds, will be set out in IAAs. The Hub administrator would use the IAAs to set business rules regarding the processing of requests and any conditions that would apply.

AGD anticipates that it would develop templates for the IAAs. These are likely to be on a sector-by-sector basis, for example there would be an IAA for Road Agencies, another for Police Agencies, etc. AGD advised that it might provide advice on the IAAs but did not expect to have a role in vetting or approving the content of the agreements.

The fact that the proposed arrangements do not contemplate that IAA would be approved by AGD was a concern for Privacy Commissioners, particularly in light of the issues noted above with respect to the difficulties in multi-agency cross-jurisdictional governance arrangements. IIS agrees that AGD should approve the IAAs.

AGD is trying to create the Hub with a set of assurances that it will be appropriately used and it is difficult to see how these can be delivered without AGD, or another independent body, taking a proactive role to ensure the intent of the IGA is not watered down.

14.AGD or Independent approval of agreements between participating agencies

(a) IIS recommends that the Interagency Agreements between participating agencies, together with the IGA that will authorise information sharing via the Hub, should be subject to approval by AGD or by another independent body such as the Australian Privacy Commissioner before use of the Hub can proceed. If a body such as the Privacy Commissioner has this role, it should receive dedicated resourcing for this function.

(b) IIS further recommends that AGD take steps to ensure that the number of agreements does not reach the point where the sheer number adversely impacts transparency and community understanding of the system as a whole. These steps could include, as AGD is contemplating, standard agreements for groups of participating agencies or specifying the requirements in legislation rather than agreements.

IIS understands that AGD is contemplating a systematic review of the Hub's operations once it is fully rolled out. IIS supports this approach and in particular the inclusion of key privacy issues in terms of reference for the review that address the issues identified in the discussions above about the

governance and effective operation of the Hub.

15. Regular systemic review of the Capability and associated information sharing arrangements

(a) IIS recommends that there is at least a three-yearly systemic review of privacy impacts around the sharing of facial biometric information by participating agencies through the Hub. The findings of the review should be made public to the extent possible. The review should:

(i) Include the activities of the Hub and the participating agencies at both individual agency level and holistically

(ii) Quantify the increase in the use of facial biometrics amongst those agencies with legal authority to use the system

(iii) Quantify actual benefits realisation

(iv) Assess extent to which the Hub itself is affecting privacy outcomes, including because the system performs less well than expected or has been subject to any significant data security breaches

(v) Assess the efficacy of responses to citizen issues with data accuracy and use, including but not limited to experiences with complaint handling

(vi) Assess the extent of community knowledge of the system, community reactions and impacts on privacy viewed broadly

(vii) Assess the effectiveness of the governance arrangements, particularly in relation to decision-making, oversight and accountability

(viii) Assess if the relevant oversight bodies are resourced for the functions and report if they are able to cooperate effectively.

6.4 Issues for Hub implementation including by State and Territories

In this course of the PIA IIS identified some risks that were out of scope. Many of these were also raised in the discussions with Privacy Commissioners and these are noted at Section 4 above. IIS expands on two significant issues here for consideration as the Hub design and implementation progresses.

- The Hub design emphasises that one-to-one verification in the context of service delivery will only occur with the individual's consent. However, in discussions it was apparent that in some cases individuals would be *informed* that their information would be disclosed to various agencies for purposes including verification of details through biometric matching and given little if any practical alternative but to accept. While technically consent might be able to be 'implied' if the individual proceeded, IIS suggests such a process is out of step with better practice concepts of consent.

  The Privacy Commissioner meetings also saw this as an issue. They questioned the nature of the consent for verification matching and whether individuals actually have real

choices, including whether it is more appropriate to recognise that compulsion is involved (or at best, very little real choice). In such cases IIS considers that it is preferable to not seek to rely on consent. The APPs permit disclosures that are for the purpose for which the information was provided or for related and expected purposes. If relying on these provisions in the APPs agencies would usually be expected to provide notice to ensure the disclosure is apparent. Where individuals have less choice, accountability and incident handling arrangements should be strengthened accordingly.

- As discussed at Section 6.2.4 IIS understands that AGD and participating agencies will generally be discouraging the capture and further use of images or biographic data returned following a request unless this is clearly intended in the nature of the request and surrounding processes. A number of strategies will be used to combat this risk. As flagged in the earlier discussion, IIS considers that, to complement those strategies, agencies should consider including a stamp on an image.

6.5 Operation/governance of the Hub if (hypothetical) future scope of NFBMC and governance of change

This PIA focuses on the design and operation of the Hub and its related governance arrangements. The use of the Hub, and how that use might expand and extend over time, is outside the scope of this PIA. IIS does understand, as flagged elsewhere in this report, that the initial implementation of the Hub is to be reasonably tightly targeted on law enforcement, national security and specified service provision. However, it is clearly envisaged that the Hub will scale out to volume and IIS considers that some of the risks will only become material at greater volumes than in the initial implementation.

IIS considers that changes beyond the initial scope or objectives should be subject to a detailed governance process, which could include but would not be limited to a PIA. The Privacy Commissioner discussions also identified this as an important issue. Matters that might trigger such a governance process would include:

- Increased potential for tracking or surveillance
- Unexpected changes in scope that are likely to be unwelcome to individuals
- Retention or transmission of biometric templates
- Potential for design to allow for retention of biographic and biometric data
- Private sector use of the Hub
- The addition of additional modalities (finger print, thumb print, iris, voice print)
- Involvement of further service delivery agencies (outside major data suppliers such as Driver Licence agencies, Passports and Immigration when issuing or managing identities and identity documentation)
- Service delivery potential impact on daily life increases very significantly.

IIS understands that under the proposed governance arrangements the LCCSC would need to endorse any changes in the NFBMC's scope or operations and that the NISCG would be the likely body to consider proposals.

16. Governance of changes to the Hub and associated information flows

(a) IIS recommends AGD, the National Identity Security Coordination Group or the Ministerial Law Crime and Community Safety Council, develop a governance process that would be triggered by any proposals that represent a significant change in the scope or operation of the Hub. The process should include:

(i) A broad consideration of costs as well as benefits

(ii) A commitment to a wide consultation process, including public consultations, to the extent possible

(iii) The inclusion of citizen perspectives beyond law, justice and national security agencies.

7. Appendix 1 – Background materials and consultations

7.1 Project and policy documents reviewed for the PIA

Documents provided for the PIA
Draft Intergovernmental Agreement on the sharing and use of facial biometrics
Glossary of Terms
Hub governance arrangements (Identifies the bodies involved and describes their roles and responsibilities
Interoperability Hub Solution Outline June 2015
Interoperability Hub: User Scenarios
NFBMC – Interoperability Hub: Assessment of Utility and Stakeholder Requirements Final Report (Draft) (excluding Appendices) by Deloitte for AGD
NFBMC – Non-Functional Requirements
NFBMC Blueprint
NFBMC Concept of Operations
Project Schedule
Promoting Interoperability of facial biometric systems – scoping study (final) by Biometix for AGD
Security and Access model
Statement of Outcomes (internal AGD Policy Document)

7.2 Meetings held with privacy regulators

Meetings held with Privacy Regulators	
Wednesday 8 July 2015	
Office of the Australian Information Commissioner	Timothy Pilgrim, Privacy Commissioner, Angelene Falk, Assistant Commissioner
Office of the Information Commissioner, Northern Territory	Brenda Monaghan, Information Commissioner
Office of the Information Commissioner, Western Australia	Sven Bluemmel, Information Commissioner
Office of the Commissioner for Privacy and Data Protection, Victoria	David Watts, Commissioner for Privacy and Data Protection

Meetings held with Privacy Regulators	
Monday 20 July 2015	
Office of the Australian Information Commissioner	Ben Gollan, Assistant Director, Regulation and Strategy, Este Darin-Cooper, Director, Regulation and Strategy, Jacob Suidgeest, Director, Regulation and Strategy, Nina Yiannopoulos, Acting Assistant Director, Regulation and Strategy, Alun Thomas, Assistant Director, Regulation and Strategy
Office of the Information Commissioner	Jenny Mead, Acting QLD Privacy Commissioner, Lemm Ex, Principal Privacy Officer
Information and Privacy Commission, New South Wales	Dr Elizabeth Coombs, Privacy Commissioner, Catherine Tat, Senior Project Officer

8. Appendix 2 – possible risks against the APPs

This table considers the application of the APPs to the Hub and to those parts of the NFBMC that affect the design Hub's design. It also flags issues that might arise in the context of the Hub's operation or changes in its functions or operations.

The analysis here is high-level and intended to flag issues. The issues identified are discussed, with other privacy risks, in Section 6 above.

APP summary	Hub design risks	Flagging risks as Hub operates or there are changes in its functions or operations
Demonstrated APP compliance – practices, procedures, systems (APP 1.2)	• Hub project will not sufficiently consider the Hub's future use, and/or it will a take a compliance, rather than best practice, approach to further design	• Responsibility and Accountability for Hub will be unclear leading to gaps/inadequacies in steps to comply • Compliance with the APPs does not take into account impacts of the NFBMC as whole
Openness – privacy policies (APP 1.3 and 1.4)	• While AGD privacy policy would not necessarily need to Hub design and pilot, better practice would be to conduct these steps as	• AGD's privacy policy or other information insufficient for citizens to understand Hub's role and functions

APP summary	Hub design risks		Flagging risks as Hub operates or there are changes in its functions or operations	
		transparently as possible		
Anonymity and pseudonymity (APP 2)			•	Potentially significant increase in circumstances where individuals are required to present photo ID – raising the issues at least with respect to the spirit of APP 2
Collection – necessary, lawful and fair and direct (APP 3)	•	Hub design results in collection of more information than needed		
Dealing with unsolicited personal information (APP 4)	•	No issues identified		
Notice/Transparency (APP 5)	•	Hub design prevents or does not sufficiently allow for participating Commonwealth agencies to be satisfied, where they seek to rely on individuals being informed about disclosures, that privacy notices have been provided	•	While not a compliance issue, better practice would be for AGD to address notice/consent issues in the IAAs and in training and standards
Limits on use and disclosure (APP 6)	•	The Hub design limits agencies' discretion to decide whether to disclose information, for example by limiting their ability to assess if a disclosure is consistent with privacy principles		
	•	Hub design prevents or does not sufficiently allow for participating Commonwealth agencies to be satisfied, where appropriate, that		

APP summary	Hub design risks		Flagging risks as Hub operates or there are changes in its functions or operations	
		consent has been given before disclosing information		
Direct marketing (APP 7)	•	No issues identified		
Transborder data flows (APP 8)			•	Would need consideration if overseas organisations are given Hub access
Unique identifiers (APP 9)	•	No issues identified	•	Consideration needed on risks associated with the exchange of and/or retention of agency specific unique identifiers or of other identifiers, such as a mobile phone numbers
Quality/Accuracy (APP 10)	•	Risk that Hub design introduces or contributes to agency data quality or accuracy risks	•	Risk that Hub operation or Governance arrangement do not give sufficient emphasis with identifying and dealing with quality or accuracy issues at the Hub or in the NFBMC as a whole
Storage and security (APP 11.1)	Risk that Hub design will not meet 'reasonable steps' to protect personal information			
Retention (APP 11.2)	Risk that Hub will retain metadata longer than is necessary			
Access and correction (APPs 12, 13)	Hub design intended to exclude retention of personal information other than metadata.		The metadata held in the Hub would not by itself identify any individual but it may be needed to assist agencies comply with access requests	

INFORMATION
INTEGRITY
SOLUTIONS

Information Integrity Solutions Pty Ltd

Level 3, 53 Balfour Street, Chippendale, Sydney NSW 2008 Australia
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898