Australian Government
Attorney-General's Department

December 2015

Preliminary Privacy Impact Assessment of the National Facial Biometric Matching Capability - Interoperability Hub

Attorney-General's Department Response

Identity crime is one of the most common crimes in Australia, costing an estimated $2bn p.a. It is also a key enabler of organised crime and terrorism.

The Document Verification Service (DVS) is an essential part of the government's efforts to combat identity crime. The DVS is a secure, online system that enables organisations to verify information on identity documents against the records of the document issuing agency. As a key initiative of the National Identity Security Strategy agreed by the Council of Australian Governments (COAG) in April 2007, the DVS is managed by the Attorney-General's Department (AGD) on behalf of the participating Commonwealth, state and territory document issuing agencies. Use of the DVS is growing significantly, particularly since it was made available to the private sector in 2014. There are now more than 30 government agencies and over 190 businesses using the service (as at August 2015). The DVS was designed to help prevent the use of fake identities – not necessarily cases involving the theft or takeover of a real person's identity.

The Australian Government is augmenting the DVS with a National Facial Biometric Matching Capability to enable government agencies to better use facial images to detect and prevent this more sophisticated type of identity fraud, while maintaining robust privacy safeguards. This capability will link the facial recognition systems of participating agencies via a network in which images may be shared, on a query and response basis, via a central exchange or interoperability hub (Hub). In doing so the Hub does not store any personal information. This 'hub and spoke' based approach offers a range of privacy and other benefits, when compared to alternative models such a centralised biometric database.

The functions of the Hub are being designed to enable agencies to participate in a range of new identity verification and related services (collectively referred to below as 'the Services') to complement the DVS:

- a *Face Verification Service* (FVS) to enable agencies to verify a person's identity by matching their photo (on a one-to-one basis) against an image on one of their government records, such as a passport photo
- a *Face Identification* Service (FIS) to enable agencies to match a photo of an unknown person against multiple government records (on a one-to-many basis) to help establish their real identity, and
- an *Identity Data Sharing Service* (IdSS) to enable agencies to share images and/or related biographical data securely and in a more auditable way than current ad hoc arrangements.

Consistent with the objectives of the National Identity Security Strategy, AGD is working with states and territories, via the COAG Law Crime and Community Safety Council (LCCSC) and Transport and Infrastructure Council (TIC) respectively, to explore the scope for police and road agencies to participate in the Capability. Arrangements to support state and territory participation are being developed in the form of an intergovernmental agreement which will outline the policy, legislative, funding and governance arrangements to support the Capability; and will be supported by data sharing agreements between participating agencies.

AGD commissioned a preliminary privacy impact assessment (PIA) on the design of the Hub that was undertaken independently by Information Integrity Solutions Pty Ltd (IIS). In its report, IIS makes 16 recommendations on the design and governance of the Hub, all of which AGD has accepted either in whole or in part. Details of AGD's response to these recommendations are provided below.

RECOMMENDATION	RESPONSE
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.	**Accept** AGD is committed to maintaining robust privacy safeguards in the design, implementation and ongoing management of the Hub and its Services.
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 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 in terms of the number and nature of participating organisations, the volume and nature of information exchanged and the potential impact on privacy.	**Accept** AGD will implement this recommendation by adopting a 'Privacy by Design' approach that seeks to limit any privacy impacts, as far as practicable, and ensure that they are reasonable and proportionate to the objectives of the capability. This approach will reflect a broad view of the concept of privacy, in addition to ensuring compliance with privacy laws. Consistent with this approach, the governance arrangements for the Services will take into account the initial and future scope of information sharing through the Hub. These arrangements will include an IGA between the Commonwealth and states and territories, with oversight by the LCCSC which includes ministers with portfolio responsibility for privacy within each jurisdiction.
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	**Accept** No biographic or biometric information can or will be stored in the Hub. However in order to ensure that the Services are operating effectively and are only accessed for legitimate purposes, certain types of transaction data must be collected for audit and control purposes. AGD will implement this recommendation by ensuring that only the minimum amount of such data required for these purposes will be collected. Example categories of these data include: • transaction number • requesting and receiving agency

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.	• pseudonymous user ID of requesting officer • type of function performed • purpose and authorisation • time and date, and • numerical 'pointers' that can be used to facilitate audits of the images shared between agencies, without making those images or other personal information accessible to AGD as manager of the Hub. These data will only be retained for the minimum period of time needed for efficient and effective operation of the Services and will only be made available to the transacting agencies or relevant oversight bodies.
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.	**Accept** AGD will implement this recommendation by designing the Hub in a way that enables agencies to include details of the purpose and authority to share images as part of information sharing/matching requests. This will be supported by formal interagency data sharing agreements between participating agencies that will outline the purpose and authority for information sharing to be facilitated through the Hub. In entering into these agreements, agencies disclosing information will be free to negotiate the terms and conditions for the release of that information to requesting agencies. Agencies will be required to enter into these agreements before being provided with access to the Services.
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	**Accept** AGD will implement this recommendation through arrangements to ensure that access to the Services will only be provided to authorised individuals within participating agencies, and that individual users will be required to re-confirm their need and authorisation to use the Services at regular intervals. Under the proposed IGA, agencies participating in the Services should provide appropriate training to personnel using the Services, including

(ii) Policy and procedures on the issue of image caching by agencies' online systems. (c) IIS recommends that AGD, in developing templates for interagency data sharing agreements, 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.	training on privacy obligations, security awareness and employment and secrecy obligations. Access to Services will be conditional on Agencies establishing procedures for the management and training of nominated users in accordance with the interagency data sharing agreements. Agencies will be encouraged to ensure that the caches of any online systems connected to the Hub are cleared of images and other personal information at the conclusion of each session. Where it is technically feasible, caches will be cleared automatically by the Hub on a regular basis. Agencies' compliance with these and other requirements will be the subject of regular audits, performed by or in consultation with agencies holding facial images, which will be a condition of Agencies' access to the Services.
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.	**Accept** AGD will implement this recommendation through arrangements that limit access to the FIS to appropriately authorised and trained users within law enforcement and security agencies or specialist fraud prevention areas within agencies that issue passports, immigration and citizenship documents and driver licences. AGD acknowledges that the FIS has a greater potential impact on the privacy of individuals. Further, the risk of accidental or unauthorised disclosure of certain protected identity information through this Service needs to be actively managed.
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.	**Accept** AGD is adopting a 'Privacy by Design' approach to the development of the Services. AGD will continue to commit to best practice privacy principles, beyond strict legislative compliance, as part of the governance framework as the Services are implemented and move to 'business as usual' processes. For example, under the proposed IGA any consideration of significant new

	policy matters by the LCCSC and the officials-level body the National Identity Security Coordination Group (the Coordination Group) must involve a consideration of privacy impacts and the broader public interest. In addition, as a condition of access to the Hub, agencies will be required to undertake PIAs to assess the privacy impacts of each information flow that will result from use of the services.
8. **Benefits assessment to take account of privacy governance costs** (a) IIS recommends that in developing the methodology for identifying and costing benefits AGD should also bring into account in all costs involved, including costs of privacy governance such as: (i) Participating agency compliance and monitoring and audit costs (ii) Resourcing of privacy regulators and other oversight bodies (iii) Assistance to individuals and the community and complaint handling.	**Accept in part** AGD notes the benefits and costs associated with use of the Services will accrue primarily with the Commonwealth, state and territory agencies that use them, rather than AGD. A benefits assessment using the methodology recommended will therefore require close engagement and input from participating agencies to complete. AGD will implement this recommendation by developing a methodology to assess the costs and benefits of the Services that includes consideration of privacy impacts and oversight costs. Developing a methodology for assessing costs to privacy regulators will add complexity to this process and will require input and agreement from all jurisdictions.
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 transparency and community engagement approach to support the introduction of the Hub.	**Accept** AGD is committed to implementing and operating the Services in a transparent manner to help build and maintain public confidence in the Government's efforts to combat identity crime. On 9 September 2015, the Minister for Justice publicly announced the government's establishment of the capability. The Minister's announcement indicated the broad scope of the capability and its Services, foreshadowing that an initial FVS would commence operation in mid-2016. In addition to publishing this PIA and this response, AGD will also make available details of the policies and agreements that support agencies participation in the Services. Further, AGD will require agencies to publish,

	on an annual basis, information on the outcomes of audits of their participation of the Services, except to the extent that any information published would compromise security of the system.
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.	**Accept** AGD will implement this recommendation by requiring agencies to publish details of the interagency data sharing agreements that support their participation in the Services. As the manager of the Hub, AGD will maintain a published register of these agreements. Agencies will be expected publish these agreements, wherever possible, unless they contain information that is not suitable for public release, in which case details of the agreements will be made publicly available to the extent possible.
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 so it will be quite clear when a change in 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, would move beyond the initial scope and therefore trigger further privacy assessments.	**Accept** AGD will implement this recommendation through the proposed IGA which sets out the initial scope of the Services. The IGA also sets out a process by which changes in the nature or scope of the Services may be implemented. The LCCSC is ultimately responsible for making decisions on significant new initiatives (such as the sharing of other types of biometric information or the use of the FVS by the private sector). The LCCSC must consider the impact of the initiative on privacy and the public interest as part of its decision making process.
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'	**Accept in part** AGD acknowledges importance of ensuring that there is a public interest test in key decisions on the operation of the Services and considers that this can be achieved through proposed governance arrangements.

perspectives.	Under the proposed IGA, the officials-level Coordination Group will be responsible to the LCCSC for the operation and governance of the Services. Membership of the Coordination Group includes a representative of the Office of the Australian Information Commissioner who acts as an independent observer or adviser on privacy issues. State and territory representatives will be expected to consult with their respective privacy commissioners and/or ombudsmen in exercising their responsibilities for oversight of the Services. At the ministerial level, responsibility for oversight of the Services will rest with the LCCSC, a body comprising ministers with portfolio responsibility for privacy and/or human rights. The proposed IGA requires that, in considering any significant new initiatives relating to the Services, the LCCSC must consider the impact of the initiative on privacy and the public interest.
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 facilitate 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	**Accept in part** AGD supports the intent of this recommendation and will implement it through an IGA that provides for: • a representative of the Office of the Australian Information Commissioner to act as an independent observer or adviser on the officials-level Coordination Group responsible to ministers for the delivery and oversight of the Services; • annual published audits of agencies' use of the Services, funding for which will be the responsibility of each jurisdiction; • agencies maintaining accessible and effective mechanisms for dealing with any complaints relating to the Services, consistent with privacy and other relevant legislation; and • each jurisdiction accepting responsibility for resourcing of privacy regulators or other relevant bodies to oversight the participation of its agencies in the Services. AGD acknowledges that any legislative impediments to cross-jurisdictional cooperation and information sharing between oversight bodies may have an impact on the regulation and oversight of agencies' use of the Services.

sharing between oversight bodies where information is shared between jurisdictions (v) Require participating agencies have in place well resourced 'safety net' mechanisms to effectively support individuals adversely affected by the use of Hub and to respond efficiently and respectfully to any complaints.	However, the oversight of cross-jurisdictional information sharing is broader than the Services and as such would be more appropriately dealt with outside of the proposed IGA.
14. **AGD or Independent approval of agreements between participating agencies** (a) IIS recommends that the Interagency Agreements between participating agencies along 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 also be separately resourced 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.	**Accept in part** AGD supports the intent of this recommendation to minimise the potential for information sharing that unnecessarily impacts on the privacy of individuals. To help manage this risk, AGD will make access to the Services conditional on agencies entering into agreements that: • outline the legislative basis on which the proposed information sharing is to be conducted: • are informed by a PIA, the outcomes of which should be published; and • meet annual auditing and any other requirements contained in the IGA or otherwise determined by the Coordination Group. AGD will develop a standard template for interagency data sharing agreements and will encourage and assist agencies to consolidate the number of agreements involved in the provision of the Services. For example, this could be achieved through the development of consolidated agreements covering all state and territory police and road agencies respectively. AGD will also retain discretion not to provide access to the Services, or to suspend or terminate access to the Services, on the grounds that an Agency is suspected or found to be in breach of its privacy obligations. This discretion will be exercised in accordance with any procedures developed and maintained by the Coordination Group. For example, this discretion may be exercised upon receipt of a complaint from a privacy regulator or oversight body, or upon a request from an agency from which information is provided.

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 of the sharing of facial biometric information of 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 response 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 that they are able to cooperate effectively.	**Accept** AGD supports the intent of this recommendation and will implement it through an IGA that provides for a review of the Services after three years. The detailed terms of reference for this review will be determined at that time, informed by this recommendation and the subsequent experience of agencies' participation in the Services. In broad terms, the review will assess: • the effectiveness of the Services in progressing the objectives of preventing identity fraud, supporting law enforcement, upholding national security, promoting road safety and streamlining service delivery, while maintaining robust privacy safeguards • the effectiveness of the governance arrangements, and • any privacy impacts and effectiveness of privacy safeguards in protecting the personal information of individuals.
16. **Governance of changes to the Hub and associated information flows** (a) IIS recommends AGD, the National Identity Security	**Accept** AGD will implement this recommendation through an IGA that provides for governance processes that require decisions on significant changes or new

	Coordination Group or the Law Crime and Community Safety Council, develop a governance process that would be triggered by proposals for significant changes 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, including public consultations, to the extent possible (iii) The inclusion of citizen perspective beyond law, justice, national security agencies.	initiatives relating to the Services to be informed by consideration of benefits and costs, including privacy impacts and the broader public interest. Where possible, this will be informed by wide consultation with a range of non-government stakeholders.