Response to the Privacy Impact Assessment of the National Driver Licence Facial Recognition Solution

Background

On 5 October 2017, the Council of Australian Governments entered into an *Intergovernmental Agreement on Identity Matching Services* (the IGA) to facilitate the secure, automated and accountable exchange of identity information, with robust privacy safeguards, in order to prevent identity crime and promote law enforcement, national security, road safety, community safety and service delivery outcomes. The IGA outlines the terms of state and territory participation in new facial biometric matching services (Face Matching Services). This includes the establishment of a National National Driver Licence Facial Recognition Solution (NDLFRS), to be hosted by the Commonwealth on behalf of the states and territories, to help make available driver licence images via the Face Matching Services.

In February 2018, the Commonwealth introduced the Identity-matching Services Bill 2018 to strengthen the legal basis for the Commonwealth Department of Home Affairs to operate the NDLFRS, and a separate Interoperability Hub, as the primary technical systems supporting the Face Matching Services.

The IGA provides for a Face Matching Services Participation Agreement (Participation Agreement) to provide a legally binding framework within which participating agencies will negotiate details of data sharing arrangements, so that these arrangements meet minimum privacy and security safeguards in order to support information sharing across jurisdictions. To complement the Participation Agreement, a separate NDLFRS Hosting Agreement is being put in place between the Department of Home Affairs (as the NDLFRS Hosting Agency) and each state and territory road agency to outline the terms on which data will be hosted in the NDLFRS.

The IGA vests ministerial responsibility for oversight of the Identity Matching Services, including the Face Matching Services, with the Ministerial Council for Police and Emergency Management (MCPEM). An officials-level National Identity Security Coordination Group (NISCG) is accountable to the MCPEM for the effective delivery and management of the Identity Matching Services.

Scope of the privacy impact assessment

Information Integrity Solutions Pty Ltd (IIS) was commissioned to conduct an independent Privacy Impact Assessment (PIA) of the proposed design, operation and governance of the NDLFRS.[1] This assessment was undertaken in consultation with the Australian Information Commissioner and state and territory privacy commissioners (or equivalents) and was completed in December 2017.

The PIA found that serious consideration was being given to the privacy risks emerging in the development of the NDLFRS; and that most of the risks identified were likely to be managed via the complementary set of strong privacy and security controls that were being proposed.[2]

The PIA makes a total of 18 recommendations for a range of measures to strengthen the governance framework and privacy safeguards in relation to the NDLFRS.

Response to the privacy impact assessment

As the body responsible to ministers for the Identity Matching Services, including the NDLFRS, the NISCG has developed a response to the recommendations of the PIA on behalf of all jurisdictions. This response accepts [10] of the PIA's recommendations in full and the remaining [8] recommendations in part. Further information on the response to each recommendation is below.

---

[1] The PIA was commissioned by the Attorney-General's Department. Since that time, lead responsibility for the Identity Matching Services has transferred to the Department of Home Affairs.

[2] IIS, *NDLFRS Privacy Impact Assessment*, November 2017, para 1.1, p. 7.

RECOMMENDATION	NISCG RESPONSE
Recommendation 1 – Ensuring State and Territory Road Transport Agencies (RTAs) control NDLFRS information and individual rights are maintained IIS recommends that AGD ensure that: • Any changes to the NDLFRS administrative or legal arrangement that could affect the extent to which the states and territories remain in control of information in their partitions of the NDLFRS should be subject to a transparent PIA process • The application of privacy and FOI law to NDLFRS data in AGD hands, including the respective roles and responsibilities for the Commonwealth and states and territories, should be clarified in law or in the IGA and legally binding participation and/or hosting agreements. • Individuals are not disadvantaged by any inadvertent impacts of the legal provisions or administrative approach, for example, on individuals' right to pursue a privacy complaint under a state or territory privacy law.	**AGREE** Any change to the technical design of the NDLFRS or to the legal or administrative arrangements supporting the system that could materially impact a state or territory's ability to control access to their information will be subject to a further privacy impact assessment. The IGA and NDLFRS Hosting Agreement explicitly acknowledge that identity information held within the NDLFRS will be subject to applicable Commonwealth legislation including the *Freedom of Information Act 1982* and the *Privacy Act 1988*. The NDLFRS Hosting Agreement requires Road Agencies to comply with applicable privacy legislation of their jurisdiction, or if there is no such privacy legislation in its jurisdiction, the Road Agency will be required to comply with the Australian Privacy Principles (APPs) in the *Privacy Act 1988*. The NDLFRS Hosting Agreement also acknowledges that the Hosting Agency does not have access to the identity information provided by Road Agencies into the system and, therefore, requires Road Agencies to take responsibility for addressing requests under applicable privacy or freedom information laws to access or correct personal information held within the NDLFRS. This Agreement will be supported by guidelines for responding to freedom of information requests relating to data held within the NDLFRS which will be developed between the Hosting Agency and Road Agencies.
Recommendation 2 – Transparency and information for individuals IIS recommends that AGD work with the NISCG and participating organisations to ensure that the IGA or the NDLFRS Hosting Agreement include non-discretionary requirements for RTAs to provide explicit up-front notice to future driver licence applicants about the Commonwealth's	**AGREE** The IGA provides that Road Agencies will take all reasonable steps to notify individuals, when applying for new or renewed driver licences, that the personal information being collected by the Road Agency may be disclosed for the purposes of biometric matching through the NDLFRS for

RECOMMENDATION	NISCG RESPONSE
collection of driver licence images for biometric face matching for law enforcement, national security and other purposes. In addition, IIS recommends that either AGD or RTAs take proactive steps to notify individuals whose information is already held by RTAs about the inclusion of their information in the NDLFRS. This could involve mail-outs to individuals and/or a public education campaign. IIS also recommends that AGD develop and disseminate information, for example in its privacy policy, and via its website, or brochures distributed by RTAs, that provides specific details on the information that would be collected for the NDLFRS and how it stored and used and the associated privacy safeguards. Information about how individuals can seek help to resolve any identity problems arising as a result of use of the NDLFRS should be included.	law enforcement, national security and other purposes. Similarly, the NDLFRS Hosting Agreement provides that Road Agencies must notify individuals that their identity information has been provided to the NDLFRS. Information on the NDLFRS, including what personal information the system contains, associated privacy safeguards, and the avenues available to individuals for resolving problems or complaints relating to the operation of the NDLFRS, will be made publically available via a government website.
Recommendation 3 – Requirements for consent based access to NDLFRS IIS recommends that AGD work with the NISCG and participating agencies to ensure that where organisations are permitted to use the Face Verification Service (FVS) to access facial images from the NDLFRS on the basis that the individuals have given their consent: • The consent must be express, freely given and fully informed • Consistent with the Commonwealth Digital Service Standard, there must be a viable alternative method available for individuals to authenticate or verify their identity • This requirement is included in the proposed legislation for the NFBMC.	**AGREE IN PART** Where organisations are using the services on the basis of consent, this consent must be obtained in accordance with relevant legislation, including the *Privacy Act 1988* (Cth) which is applicable to Commonwealth agencies and private sector organisations; and state and territory privacy laws which are applicable to state and territory agencies. The IGA and Participation Agreement include requirements for an organisation's use of the services to be subject to a privacy impact assessment (PIA). These PIAs provide an opportunity to examine the way in which organisations obtain consent and to make recommendations on how processes for obtaining consent might be improved. Under the Participation Agreement these PIAs are required to be published to the extent possible, taking into account security considerations. The Commonwealth Identity-matching Services Bill 2018 does not contain requirements relating to the way in which users of the services obtain consent from individuals. The purpose of this Bill is to authorise the

RECOMMENDATION	NISCG RESPONSE
	Department of Home Affairs to operate the technical systems, including the NDLFRS, which support the Identity Matching Services. Collection of information from individuals, including processes for obtaining consent, is governed by other legislation including Commonwealth, state and territory privacy legislation.
Recommendation 4 – Process to handle false negative matches IIS recommends that AGD work with road transport agencies to develop a strong privacy approach to the handling of 'no match' or error responses following a face match request using the NDLFRS by doing such things as: • Undertaking risk assessments to identify issues that might arise for individuals • Encouraging consistent business processes across all jurisdictions • Identifying agreed benchmarks for resolving issues and ensuring resources are available to meet the benchmarks • Requiring each jurisdiction to have resources available to resolve issues for their own customers and to respond to requests from other jurisdictions within a reasonable time frame. Each jurisdiction should also provide up-to-date details for a contact person to facilitate resolution of requests. IIS also recommends that AGD work with RTAs to ensure that individuals do not have to contact multiple agencies to resolve issues arising from use of face matching services. For example, AGD could coordinate a single point of contact for inquiries and resolution of match failures or could require the first agency contacted to coordinate resolution of the problem. The approaches should be reflected in the IGA, amending legislation, Participation Agreement, NDLFRS Hosting Agreement and user guidance.	**AGREE IN PART** The IGA requires states and territories and the Commonwealth to maintain accessible and effective mechanisms for responding to any public complaints relating to use of the Identity Matching Services, including the Face Matching Services. The Participation Agreement requires agencies to respond to any enquiries or complaints by members of the public, or to refer the complaint to another agency where appropriate. The NDLFRS Hosting Agreement provides that the NDLFRS Data Hosting Agency will be the central point of contact for queries or complaints. It also provides that each Road Agency must ensure that it has sufficient resources, including by providing to individuals a help desk function, to govern their handling of complaints and queries from individuals relating to the NDLFRS. This Agreement will be supported by guidelines for handling of match failures, which will be developed between the Hosting Agency and Road Agencies. These guidelines will reflect the role of the NDLFRS Hosting Agency, as a central point of contact and coordination for inquiries and resolution of match failures. It is not considered necessary to include these requirements in the Commonwealth's Identity-matching Services Bill 2018, as they can be addressed effectively in related agreements and guidelines.

RECOMMENDATION	NISCG RESPONSE
Recommendation 5 – Monitoring data accuracy and matching processes IIS recommends that AGD work with the NISCG to monitor and report on the frequency and nature of face matching fails arising from use of the FVS and One Person One Licence Service (OPOLS) and the way state and territory agencies or other users handle such fails. They should take steps to identify underlying causes for the match fails and change policies or procedures as needed to minimise the impact on individuals.	**AGREE** The NISCG will explore the scope to establish a research project to examine FVS and OPOLS matching results, with a view to identifying the underlying causes of matching fails and recommending any changes to policies and procedures that may be needed to address this issue in order to minimise the impact on individuals.
Recommendation 6 – Formal data retention policy IIS recommends that AGD in consultation with the jurisdictions develop a data retention policy for the NDLFRS that provides for requests or queries, templates and audit logs and other related information to be retained for the minimum time possible. Unless there are good reasons for a different approach these should be similar to the Document Verification Service (DVS) retention times or better.	**AGREE** Data held within and/or generated by the NDLFRS will only be retained for the minimum period of time that this necessary: to support the operation of the system, including auditing and oversight; and for participating agencies to carry out the purpose for which the information was collected, and meet legislative requirements for the retention of government records. These requirements are reflected in the Participation Agreement (for agencies accessing NDLFRS data) and the NDLFRS Hosting Agreement (for the Hosting Agency). The Department of Home Affairs will develop a supporting record keeping policy in relation to the data it holds as operator of the NDLFRS.
Recommendation 7 – Clarity on roles and processes in responding to requests for access to information IIS recommends that AGD and participating agencies have detailed agreements on the handling of individual requests for access to, or correction of, driver licence information that are made to AGD as the NDLFRS manager or host. IIS recommends that if any legal impediments to the flow of information to meet these requests be identified, suitable amending legislation be introduced by the affected jurisdiction, working closely with AGD to ensure consistency. IIS also recommends that AGD's NDLFRS help desk staff have instructions, based on worked out scenarios, on how to assist individuals.	**AGREE IN PART** The NDLFRS Hosting Agreement provides that the Hosting Agency will be the central point of contact for queries or complaints. Under the Hosting Agreement, Road Agencies acknowledge that the Commonwealth Data Hosting Agency does not have access to personal information held in the NDLFRS. The Hosting Agreement provides that Road Agencies will take responsibility for addressing requests for access to or correction of an individual's personal information under the jurisdiction's freedom of information or privacy legislation.

RECOMMENDATION	NISCG RESPONSE
	The Hosting Agreement also requires each Road Agency to ensure that it has sufficient resources, including by providing a help desk function, to manage complaints and queries from individuals relating to the NDLFRS. This Agreement will be supported by guidelines for responding to access to information requests, which will be developed between the Hosting Agency and Road Agencies. These guidelines will reflect the role of the Hosting Agency, as a central point of contact and coordination for such requests, and will be supported by local guidelines developed by each Road Agency. Should any legal impediments to the flow of information to meet these requests be identified, it will be a matter for each affected jurisdiction to consider the need for amending legislation.
Recommendation 8 – Proactive and coordinated data breach management IIS recommends that AGD work with the NISCG to ensure that the IGA, the NDLFRS Hosting Agreement and/or the Participation Agreement as appropriate, includes requirements on all participants for the notification and handling of significant data breaches that could affect the operation of the NDLFRS. The requirements should provide clarity about who would be responsible in the event of data breach and should ensure that the relevant privacy regulator and affected individuals should be notified about significant breaches in the same circumstances as in the Privacy Amendment (Notifiable Data Breaches) Act 2017.	**AGREE** The IGA includes an acknowledgement that any unauthorised disclosure of identity information via the NDLFRS may, depending on the circumstances of the disclosure, require notification in accordance with the Notifiable Data Breach Scheme established under the *Privacy Act 1988* (Cth). The Hosting Agreement requires the Hosting Agency to take reasonable measures to mitigate the risks associated with any data breach and comply with relevant laws, including the *Privacy Act 1988*. Road Agencies are required under the Agreement to provide reasonable assistance and information to the NDLFRS Data Hosting Agency in managing any data breach. The Hosting Agreement also requires participating agencies to develop a plan for responding to data breaches.
Recommendation 9 – Benefits realisation	**AGREE**

RECOMMENDATION	NISCG RESPONSE
IIS strongly support the developments of a benefits realisation model. IIS recommends that AGD ensure that the proposed model be able to identify the benefits that accrue from the NDLFRS as well as for the NFBMC as a whole.	The NISCG will develop a benefits realisation model for the Face Matching Services that, as far as is practicable, delimits the benefits that accrue from use of data within the NDLFRS compared to the benefits of the services as a whole.
Recommendation 10 – Governance body membership IIS recommends that AGD work with the NISCG to have the NISCG membership expanded to include at least one state or territory privacy regulator in addition to the Australian Privacy Commissioner. IIS also recommends that the question of the appropriate oversight body for the NFBMC and the NDLFRS be revisited if access to services using NDLFRS data is extended to human service organisations or commercial providers.	**AGREE IN PART** The NISCG terms of reference have been revised to provide for the inclusion of a state and territory privacy commissioner. The NISCG considers that existing arrangements are adequate to oversight the use of NDLFRS data via the Face Matching Services by human service organisations and the private sector, noting that these organisations can currently access the DVS, which is also subject to NISCG oversight.
Recommendation 11 – Publication of privacy impact assessments for NDLFRS access IIS recommends that the NISCG work with the states and territories to ensure that the requirements for transparency about privacy impact assessments be non-discretionary for participating agencies. Where agencies are required to undertake privacy impact assessments in order to use the NDLFRS, the privacy impact assessment reports, and the agencies' responses, should be published. The only exceptions to the publishing requirement should be on security or national security grounds. If publication of a PIA is withheld, IIS recommends that: • These should be couched narrowly and not apply to a whole report if only some aspects are sensitive • If the whole report, or a redacted report, cannot be published a summary of the report should be published • If the agency is unable to publish the report or a report summary, it should be required to be accountable by discussing the report, and its response, with an independent body such as a privacy commissioner or ombudsman and report on the fact that this has been done.	**AGREE** The Participation Agreement requires the publication of privacy impact assessments to the extent possible, taking into account security considerations.

RECOMMENDATION	NISCG RESPONSE
Recommendation 12 – Annual reports on use of NDLFRS for Face Matching Services and OPOLS IIS recommends that the AGD work with the states and territories to identify relevant information about the use of the NDLFRS for inclusion in the proposed annual report on the use of Face Matching Services. IIS recommends that, in addition to the matters outlined in the draft IGA, this should include: • Usage of the NDLFRS as source data for the Face Identification Service (FIS), by Holding Agency and Requesting Agency, with sufficient detail to enable an understanding of the purposes for which the services are used • Usage of the NDLFRS as source data for the FVS with sufficient detail to enable understanding of the purposes for which both government bodies and private sector organisations use the service • Usage of the OPOLS with sufficient detail to enable understanding of the volume and nature of use • Indicative false negative or false positive matches and how long it takes for the matters to be resolved for individuals beyond usual processing times.	**AGREE IN PART** Under the Commonwealth's Identity-matching Services Bill 2018, an annual report on use of the Face Matching Services will need to be tabled in the Australian Parliament, covering: • in relation to the FVS, FIS and OPOLS: the relevant user agencies, number of requests in response to which information was provided, and number of times no information was provided in response to a request each service, • in relation to the FIS: the purpose(s) for which an agency used the service, and • in relation to the FVS: the number of times non-government entities requested to use the service, the number of non-government entities making requests, the number of requests in which a response was provided, and the number of requests in which a response was not provided. The NISCG agrees that this is an appropriate level of detail for the annual report. The annual reporting will not include the purposes for which entities are using the FVS, as in most cases this will be for identity verification. In addition, annual reporting will not include information on false negative or false positive matches. Given the time that will be needed to implement the NDLFRS across all jurisdictions, this will be more appropriately addressed via the review of the operation of the Identity Matching Services, to be conducted in 2020.
Recommendation 13 – OPOLS Access Policy IIS supports the framework set out in the IGA for governing access to the OPOLS. In addition to the measures proposed, and subject to state and territory PIAs, IIS recommends that all adverse decisions about licence applications, transfers and renewals should be subject to a 'human' review	**AGREE** Responses to OPOLS queries will be reviewed by staff who perform specialist identity resolution and exception handling processes warranting use of the service. Those staff must be sufficiently trained in facial

RECOMMENDATION	NISCG RESPONSE
and review processes should be designed to minimise privacy risks, inconvenience or other impacts on individuals so that they are the same as if the processes had occurred in only one jurisdiction.	comparison and other relevant areas to ensure privacy-respecting, efficient and effective use of the service. Under the IGA, the Identity Matching Services are not intended to be used as the sole basis for identity resolution. All participating agencies, including Road Agencies using the OPOLS, should ensure that appropriate review mechanisms are in place in relation to any adverse decision made on the basis of a result from an Identity Matching Service.
Recommendation 14 – Monitoring use of NDLFRS data IIS recommends that AGD ensure it has taken all reasonable steps to proactively detect any misuse of the NFBMC that could arise with the implementation of the NDLFRS including, to the extent practical, proactively monitoring audit logs of its use of the system to detect as soon as possible any nefarious or poor practices.	**AGREE** As part of the broader compliance framework for the Face Matching Services, a range of mechanisms are being implemented that will help detect and manage any unauthorised use of data held within the NDLFRS. These include annual audits of each Requesting Agency's use of the services and an annual privacy assessment of the operation of the NDLFRS, the first of which will be undertaken by the OAIC. The results of these audits will be provided to the NISCG. The Department of Home Affairs is also putting in place technical controls in the Interoperability Hub which supports the Face Matching Services to help detect anomalous or potentially suspicious transactions or patterns of transactions.
Recommendation 15 – Seamless privacy oversight and investigations IIS recommends that AGD work with the NISCG and privacy regulators in each of the jurisdictions to ensure that mechanisms and resourcing for external oversight of RTAs sharing NDLFRS data via the Face Matching Services – by privacy regulators, Ombudsmen or anti-corruption bodies – are commensurate with data flows and that any impediments to cooperation and information sharing between oversight bodies are removed. IIS further recommends that any legislative impediments to such cooperation and information sharing should be addressed, including via provisions in the proposed NFBMC legislation or in the IGA or other binding agreements for the use of NDLFRS services.	**AGREE IN PART** Under the IGA, each jurisdiction is responsible for any additional resourcing of privacy regulators and oversight bodies required to ensure that agencies in their jurisdiction can comply with the IGA=. The Department of Home Affairs is also providing funding to the Office of the Australian Information Commissioner to assist in meeting costs associated with annual privacy assessments relating to the NFBMC, including the NDLFRS.

RECOMMENDATION	NISCG RESPONSE
IIS also recommends that NDLFRS not proceed unless resourcing issues are satisfactorily addressed.	
Recommendation 16 – Review of the operation of the NDLFRS IIS recommends that as soon as possible after the NDLFRS goes live, AGD work with the NISCG, RTAs and jurisdiction privacy regulators to develop terms of reference for the proposed three-year review of the Identity matching services to ensure that issues relevant to the privacy impacts of the NDLFRS are included. The review criteria should take account of matters raised in this PIA and in further PIAs on agency, jurisdiction or private sector use of data within the NDLFRS, including: • The extent to which individuals are aware of and comfortable with the inclusion of images in the NDLFRS • Where use of NDLFRS data via the Face Matching Services is subject to consent, whether the consent processes used are best practice • The number of nature of false negative or false positive errors RTAs encounter in matching using NDLFRS data and the indicatives sources of error • Feedback from privacy regulators on any difficulties in providing effective oversight of, and privacy complaint handling arising from, RTAs' information sharing of NDLFRS data via the Face Matching Services • Benefit actually realised for the NDLFRS They should include evaluation of benefits actually realised. The NISCG should ensure that AGD, RTAs and other NDLFRS users have systems in place to collect the information for the review based on the terms of reference.	**AGREE IN PART** The NISCG agrees that the three-year review of the Identity Matching Services should consider the matters identified in this recommendation. The NISCG will develop draft terms of reference for this review as soon as practicable after access to NDLFRS information is made available across jurisdictions via the Face Matching Services. However, the NISCG considers that these terms of reference should not be finalised until the review is to commence, so as not to inadvertently limit the types of information that the review may consider or the ways in which the review may be carried out.
Recommendation 17 – Gaps in privacy safeguards where jurisdictions do not have privacy law IIS recommends that the proposed amendments to Commonwealth legislation to support the NFBMC require that agencies or organisations seeking access to face matching services relying on the NDLFRS be subject to a law, or binding scheme, that has the effect of protecting personal	**AGREE IN PART** The Commonwealth's Identity-matching Services Bill 2018 is not intended to change the legislative basis on which government agencies use these services. It is intended to authorise the Department of Home Affairs to operate the technical systems necessary to provide the services to

RECOMMENDATION	NISCG RESPONSE
information used in face matching services in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information and that there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme.	agencies which must have a lawful basis to access the services in other legislation. This recommendation is being implemented through a legally binding Face Matching Services Participation Agreement, developed pursuant to the IGA. Through the Participation Agreement, agencies in jurisdictions which do not have privacy legislation (currently South Australia and Western Australia) undertake to comply with the Australian Privacy Principles in the *Privacy Act 1988* in relation to their participation in the Face Matching Services. Should individuals wish to make a privacy related complaint in relation to the participation in the Face Matching Services of state agencies that are not subject to state privacy legislation, these complaints can be directed to the relevant oversight body in that jurisdiction. This could, for example, be a state information commissioner, ombudsman or privacy committee.
Recommendation 18 – Changes to NDLFRS IIS supports AGD's view that the governance arrangements for the NDLFRS should ensure that significant changes to the Face Matching Services relying on the NDLFRS such as new types services, new purposes or new categories of users are subject to privacy impact assessments. IIS recommends that such significant changes should also be subject to consultation with privacy regulators in all jurisdictions and with community representatives.	**AGREE** Any material changes to the scope of the Face Matching Services will be subject to a privacy impact assessment, conducted in consultation with Commonwealth, state and territory privacy regulators.