

INTERGOVERNMENTAL AGREEMENT ON IDENTITY MATCHING SERVICES

An Agreement to share and match identity information, with robust privacy safeguards, to prevent identity crime and promote law enforcement, national security, road safety, community safety and service delivery outcomes.

5 October 2017

This Agreement can be entered into by the following parties:

- The Commonwealth of Australia
- The State of New South Wales
- The State of Victoria
- The State of Queensland
- The State of Western Australia
- The State of South Australia
- The State of Tasmania
- The Australian Capital Territory, and
- The Northern Territory of Australia.

Recitals

- A. The Commonwealth, and participating state and territory governments wish to enter into this Intergovernmental Agreement (Agreement) to promote the sharing and matching of identity information to prevent identity crime, support law enforcement, uphold national security, promote road safety, enhance community safety and improve service delivery, while maintaining robust privacy and security safeguards.
- B. In entering this Agreement, the parties recognise that they have a mutual interest in facilitating the sharing of identity information, and need to work together to achieve these outcomes.
- C. The sharing of this information will be facilitated by the following Identity Matching Services under this Agreement:

Identity Matching Services		
Document Verification Service	Face Matching Services <ul style="list-style-type: none">• Face Verification Service• Face Identification Service• One Person One Licence Service• Facial Recognition Analysis Utility Service	Identity Data Sharing Service

- D. The parties acknowledge the importance of protecting the privacy of individuals, including the right under some jurisdictions' privacy laws for an individual to remain anonymous or to use a

pseudonym when interacting with governments and businesses in certain circumstances. While the sharing of identity information through the Identity Matching Services limits the right to anonymity, this limitation is reasonable, necessary and proportionate.

- E. The Identity Matching Services will help promote privacy by strengthening the integrity and security of Australia's identity infrastructure—the identity management systems of government Agencies that issue Australia's core identity documents such as driver licences and passports. These systems play an important role in preventing identity crime. Identity crime is one of the most common and costly crimes in Australia and is a key enabler of serious and organised crime. Identity crime is also a threat to privacy when it involves the theft or assumption of the identity of an individual. The misuse of personal information for criminal purposes causes substantial harm to the economy and individuals each year.
- F. On 13 April 2007, the Council of Australian Governments (COAG) entered into an *Intergovernmental Agreement to a National Identity Security Strategy*. An updated National Identity Security Strategy (NISS) was agreed by COAG in 2012 following a review of the 2007 Agreement. The overall objective of the NISS is for the Commonwealth, states and territories to work collaboratively to enhance national security, combat crime and increase service delivery opportunities through nationally consistent processes for enrolling, securing, verifying and authenticating identities and identity credentials. The Document Verification Service is a key initiative of the NISS that provides a practical means of promoting identity security across the Australian community.
- G. The NISS also recognises the potential for biometric identity management systems to help prevent identity crime and promote trust and confidence in the identity documents issued by government Agencies. The National Biometric Interoperability Framework was developed in 2012 to foster greater collaboration between Agencies using biometric systems across government. This Agreement marks an important step in implementing the National Biometric Interoperability Framework and in achieving the priorities of the NISS more broadly.

Operative provisions

The parties agree:

Part 1 Objective and scope of this Agreement

- 1.1 The objective of this Agreement is 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.
- 1.2 In accordance with the terms of this Agreement, the parties agree to promote the sharing and matching of identity information for the purposes of:
- (a) *Preventing identity crime* — the prevention, detection, investigation or prosecution of identity crime.
 - (b) *General law enforcement* — the prevention, detection, investigation or prosecution of an offence under Commonwealth, state and/or territory laws.
 - (c) *National security* — conducting investigations or gathering intelligence for purposes relating to Australia's defence, security, international relations or law enforcement interests.

Note: Section 8 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) defines 'national security' as Australia's defence, security, international relations or law enforcement interests'.
 - (d) *Protective security* — activities to promote the security of Agency assets, facilities or personnel, including but not limited to:
 - i. the protection and management of legally assumed identities, and
 - ii. security or criminal background checking.
 - (e) *Community safety* — activities to identify individuals who are at risk of, or who have experienced, physical harm, including but not limited to:
 - i. investigating individuals that are reported as missing
 - ii. identifying individuals who are reported as dead, or unidentified human remains
 - iii. identifying individuals when addressing significant risks to public health or safety, or
 - iv. identifying individuals in relation to disaster events or major events.

- (f) *Road safety*—the conduct of activities to improve road safety, including detection of unlicensed and disqualified drivers and individuals who hold multiple licences.
- (g) *Identity verification* — the verification of an individual’s identity, where this is done with the consent of the individual or as authorised or required by law, for example in the delivery of government services or for private sector organisations to meet regulatory identity verification requirements.

1.3 This exchange of identity information will be facilitated through the Identity Matching Services, which comprise:

- (a) the Document Verification Service
- (b) the Face Verification Service
- (c) the Face Identification Service
- (d) the One Person One Licence Service
- (e) the Face Recognition Analysis Utility Service
- (f) the Identity Data Sharing Service, and
- (g) any other identity matching or data sharing service developed under the auspices of this Agreement.

1.4 The scope of information sharing via the Identity Matching Services includes, but is not limited to:

- (a) the sharing of identity information held by states and territories with the Commonwealth, for use by the Commonwealth
- (b) the sharing of identity information held by states and territories with the Commonwealth, so that the Commonwealth may share that identity information with another state or territory that is a party to this Agreement, for use by that state or territory
- (c) the sharing of identity information held by the Commonwealth with the states and territories, for use by those states and territories, and
- (d) providing authorised private sector organisations with access to the Document Verification Service and the Face Verification Service for matching against identity information held by the Commonwealth, states and territories, with the consent of the individual concerned.

1.5 Any expansion of the scope of information sharing via the Identity Matching Services, as set out in clause 1.4, will only occur with agreement in writing by the parties.

Part 2 Guiding Principles

2.1 The parties agree that the Identity Matching Services should be developed and operated in accordance with the following principles:

- (a) **Privacy by design:** the design and operation of the Identity Matching Services adopt robust privacy safeguards, informed by independently conducted privacy impact assessments, developed in consultation with federal and state privacy commissioners (or equivalents), to balance privacy impacts against the broader benefits to the community from sharing and matching identity information.
- (b) **Best practice security:** the common systems supporting the Identity Matching Services adopt best practice security arrangements, in accordance with the Protective Security Policy Framework and Information Security Manual. Participating Agencies need to implement appropriate security and access controls, including audit and compliance mechanisms.
- (c) **Data providers maintain access controls:** each Data Holding Agency that provides access to identity information via the Identity Matching Services will retain control over which other Agencies may access that information. The scope and terms of this access will be set out in formal arrangements between participating Agencies.
- (d) **Data quality:** each Data Holding Agency that makes identity information available via the Identity Matching Services will take reasonable measures to maintain the accuracy, integrity and availability of that information, including measures to ensure facial images are of appropriate quality for biometric matching.
- (e) **Identity resolution by users:** the Identity Matching Services provide a tool to assist Agencies with identity based decisions, but ultimately responsibility for identity resolution decisions rests with Requesting Agencies that receive matching responses.
- (f) **Non-evidentiary system:** the results of the Identity Matching Services are not designed to be used as the sole basis for ascertaining an individual's identity for evidentiary purposes.
- (g) **Protect legally assumed identities:** the Identity Matching Services are designed to mitigate the risk of unintentional or deliberate disclosure of legally assumed or other protected identities.
- (h) **Robust accountability:** implementation and operation of the Identity Matching Services will be overseen by robust governance arrangements at the national level, including oversight by the Coordination Group and appropriate ministerial council.

Part 3 Definitions and interpretation

3.1 Unless otherwise specified, the following terms and definitions are used throughout this Agreement:

Access Policy means a documented set of requirements approved by the Coordination Group that an Entity must comply with in order to access the Identity Matching Services. There are separate access policies for each Identity Matching Service.

Agency means any agency, government sector agency, public sector agency or public sector body as defined in the *Public Service Act 1999* (Cth) or equivalent state or territory public service legislation, including any Road Agency, law enforcement agency or relevant Commonwealth agency that is participating in or may wish to participate in any of the Identity Matching Services.

Agreement means this *Intergovernmental Agreement on Identity Matching Services* and any Schedule to this Agreement.

Commonwealth means the Commonwealth of Australia.

Data Holding Agency means an Agency that contributes identity information used in the Face Matching Services to provide responses to queries from Requesting Agencies. For the purposes of the National Driver Licence Facial Recognition Solution, state and territory Road Agencies are Data Holding Agencies.

Data Hosting Agency means the Commonwealth Agency responsible for managing and operating the National Driver Licence Facial Recognition Solution, where it holds a replicated copy of identity information contributed by state and territory Data Holding Agencies.

De-duplicate means the process of establishing that multiple records exist for the same individual and then either consolidating or deleting matching records.

Document Verification Service (DVS) is a secure, national, online system that enables Entities to verify biographical information on identity documents against corresponding records held by document issuing Agencies.

Entity means an Agency or an Organisation that is authorised to participate in, or may wish to participate in, any of the Identity Matching Services.

evidentiary purposes means adducing information for use as evidence in a court or other judicial proceedings.

Face Identification Service means the service that enables a facial image to be compared against multiple images held on a database of government records to establish an individual's identity.

facial images includes digital photographs, live capture images, scanned photographs and other technical information related to those images (such as the time and date of capture and data capture standards used).

Face Matching Services is a collective term for the Identity Matching Services that involve facial biometric matching, namely the Face Verification Service, Face Identification Service, Facial Recognition Analysis Utility Service and One Person One Licence Service.

Face Matching Services Participation Agreement (Participation Agreement) means the legal agreement of that name made between all Agencies participating in the Face Matching Services and setting out their respective roles, rights and obligations to each other in relation to their participation in, access to and use of the Face Matching Services.

Facial Recognition Analysis Utility Service means the service that enables state and territory Road Agencies to conduct biometric matching using their own data holdings within the National Driver Licence Facial Recognition Solution.

Face Verification Service means the service that enables a facial image associated with an individual to be compared against a facial image held on a specific government record associated with that same individual to confirm that individual's identity.

Identity crime is a generic term to describe activities or offences in which a perpetrator uses a fabricated, a manipulated, or a stolen or otherwise assumed identity to facilitate the commission of a crime. Identity crime includes, but is not limited to, offences relating to the possession of, and dealing in, information or equipment used to manufacture fraudulent evidence of identity documents.

Identity Data Sharing Service (IDSS) means the service that enables the sharing of identity information between participating Agencies, on an incremental or other regular basis, to help maintain the accuracy and integrity of identity-based records. The IDSS does not involve any facial biometric or other data matching.

identity document means any document or record, whether in physical or electronic form, including words, symbols or images, that contains or incorporates identification information and that is capable of being used as evidence of identity.

identity information means information, or a document, relating to an individual (whether living, dead, real or fictitious) that is capable of being used (whether alone or in conjunction with other information or documents) to identify or purportedly identify the individual.

Identity Matching Services means the services described in Part 4 of this Agreement.

interoperability Hub means the technical system that provides a mechanism for the secure and auditable transmission of facial images and associated information between Agencies or Entities participating in the Face Matching Services.

Ministerial Council for Police and Emergency Management (MCPEM) means the body comprising Commonwealth, state and territory Ministers who have responsibility for police and emergency management and which meets from time to time as a formal council of Ministers.

law enforcement agency means any agency of the Commonwealth, state or territory governments that has responsibility for, or has powers, functions or duties in relation to, enforcement of the criminal law of the Commonwealth or a state or territory.

National Driver Licence Facial Recognition Solution means the information technology system by which facial images used on driver licences and other state and territory government issued documents can be accessed via the Face Matching Services.

National Identity Security Coordination Group (Coordination Group) means the body which is responsible to the MCPEM for the management of the Identity Matching Services.

One Person One Licence Service means the service that enables a facial image to be compared, on a constrained one-to-many basis, to other images in the National Driver Licence Facial Recognition Solution to identify whether a licence holder or applicant holds multiple licences in the same or a different identity across participating jurisdictions.

Organisation means a member of the private sector, being an individual, body corporate, partnership, unincorporated association or trust that is not an Agency and that is participating in or may wish to participate in the Identity Matching Services.

party means any of the Commonwealth, states or territories that is a party to this Agreement.

personal information has the same meaning as under the *Privacy Act 1988* (Cth). Personal information includes but is not limited to identity information.

Requesting Agency means the Agency that submits a query to a Data Holding Agency, through the Face Matching Services.

Road Agency means an Agency with responsibility for driver licencing, and includes an Agency that carries out those functions as a delegate or agent of the Road Agency.

state means the Government of a state of Australia that is a party to this Agreement.

territory means the Government of the Australian Capital Territory or the Northern Territory that is a party to this Agreement.

Transport and Infrastructure Council (TIC) means the body comprising Commonwealth, state and territory Ministers who have responsibility for transport and infrastructure and which meets from time to time as a formal council of Ministers.

Part 4 The Identity Matching Services

Document Verification Service (DVS)

- 4.1 The DVS is a secure, national online system that enables approved Entities to verify biographical information on identity documents against the corresponding record held by a document issuing or authorised Entity. The DVS has been available to Agencies since 2009, and to Organisations since 2014.
- 4.2 The DVS provides a 'yes' or 'no' response to queries as to whether certain biographical information on an identity document matches the information held on its corresponding record and that the document has not been revoked.
- 4.3 The DVS provides user Agencies and Organisations with greater confidence that information presented on identity documents is legitimate, current and not fictitious or otherwise fraudulent.
- 4.4 An Entity must have the consent of the individual to which the biographical information relates before it may verify a record via the DVS.
- 4.5 Governance of the DVS is in accordance with the policies and procedures developed and maintained by the Coordination Group.

Face Verification Service (FVS)

- 4.6 The FVS enables a facial image of an individual to be compared by an Entity against a facial image held on a specific government record associated with that same individual.
- 4.7 The FVS involves searching or matching of facial image records on a 'one to one' basis to help verify an individual's identity.
- 4.8 The FVS provides an Entity with:
 - (a) a 'match' or 'no match' response to queries as to whether an individual's facial image and purported identity match that held on a relevant government record, and/or
 - (b) the ability to retrieve a facial image of an individual held on a specific government record.
- 4.9 Before using the FVS, an Entity must have either:
 - (a) the consent of the individual associated with the facial image to be verified, gained in accordance with any applicable privacy legislation, including the *Privacy Act 1988* (Cth), or any relevant state and territory legislation; or

- (b) another legislative basis or authority to collect and use the information to be sought via the FVS.

4.10 Use of the FVS by an Entity must be compliant with the *Privacy Act 1988* (Cth), relevant state and territory privacy legislation and/or other applicable legislation.

4.11 An Agency that accesses the FVS must comply with the requirements of the Participation Agreement, including the FVS Access Policy developed by the Coordination Group.

4.12 Governance of the FVS will be in accordance with the policies and procedures developed and maintained by the Coordination Group.

Face Identification Service (FIS)

4.13 The FIS enables a facial image to be compared against multiple facial images held on a database of government records.

4.14 The FIS involves searching or matching of facial image records on a 'one-to-many' basis to help:

- (a) ascertain the identity of an individual, or
- (b) detect instances where an individual may hold multiple fraudulent identities.

4.15 The FIS provides a gallery of the highest matching facial images, as determined by the facial recognition system of the Data Holding Agency (based on a pre-configured match threshold).

- (a) In the case of the National Driver Licence Facial Recognition Solution, the facial recognition system is provided by the Data Hosting Agency.

4.16 Upon receipt of a response to a FIS request, the Requesting Agency is responsible for reviewing the facial image gallery in order to resolve the identity of the individual who was the subject of the request.

- (a) The biographic details associated with the facial images will only be released once the user selects a limited shortlist of the particular facial image or images they wish to examine.

4.17 Before receiving access to the FIS, an Agency must have a legislative basis or authority to collect and use the information to be sought via the FIS.

4.18 Use of the FIS must be compliant with the *Privacy Act 1988* (Cth), relevant state and territory privacy legislation and/or other applicable legislation.

4.19 Access to the FIS is restricted to Agencies with law enforcement or national security related functions that are approved by the Coordination Group.

4.20 Where an Agency is approved to access the FIS by the Coordination Group, each Data Holding Agency retains discretion as to whether to enter into a data sharing arrangement with the Agency.

4.21 Agencies with access to the FIS may only use the FIS for one or more of the following permitted purposes:

- (a) *Preventing identity crime* — the prevention, detection, investigation or prosecution of identity crime.
- (b) *General law enforcement* — the prevention, detection, investigation or prosecution of an offence under Commonwealth, state and/or territory laws carrying a maximum penalty of not less than three years imprisonment.
- (c) *National security* — conducting investigations or gathering intelligence for purposes relating to Australia's defence, security, international relations or law enforcement interests.

Note: Section 8 of the National Security Information (Criminal and Civil Proceedings) Act 2004 (Cth) defines 'national security' as Australia's defence, security, international relations or law enforcement interests'.

- (d) *Protective security* — activities to promote the security of agency assets, facilities or personnel, including but not limited to:
 - i. the protection and management of legally assumed identities, and
 - ii. security or criminal background checking.
- (e) *Community safety* — activities to identify individuals who are at risk of, or who have experienced, physical harm, including but not limited to:
 - i. investigating individuals who are reported as missing
 - ii. identifying individuals who are reported as dead, or unidentified human remains
 - iii. identifying individuals when addressing significant risks to public health or safety, or
 - iv. identifying individuals in relation to disaster events or major events.

4.22 The scope of the general law enforcement purpose in clause 4.21(b) does not limit the ability of the parties to share identity information between Agencies within the same jurisdiction.

4.23 An Agency that accesses the FIS must comply with the requirements of the Participation Agreement, including the FIS Access Policy developed by the Coordination Group.

- 4.24 Governance of the FIS will be in accordance with the policies and procedures developed and maintained by the Coordination Group.
- 4.25 The Coordination Group will review the definition and operation of the general law enforcement purpose in clause 4.21(b), 12 months after the FIS commences operation, and will provide a report on the outcomes of the review to the MCP EM. This review should consider whether the definition maximises the utility of the FIS for law enforcement agencies, while maintaining appropriate privacy safeguards.

One Person One Licence Service (OPOLS)

- 4.26 The OPOLS reinforces the ‘one person, one licence’ principle and helps to promote road safety by preventing driver licence fraud and sanction avoidance across jurisdictions.
- 4.27 The OPOLS enables a narrowly focused check, on a constrained one-to-many basis, of facial images within the National Driver Licence Facial Recognition Solution to identify whether a licence holder or applicant may hold another licence of the same type, in the same or different identity, in another jurisdiction.
- 4.28 The OPOLS provides a gallery of a very small number of the highest matching facial images, as determined by the facial recognition system of the National Driver Licence Facial Recognition Solution (based on a pre-configured match threshold).
- 4.29 Upon receipt of a response to an OPOLS query, the Requesting Agency is responsible for reviewing the facial image gallery in order to resolve the identity of the individual who was the subject of the query.
- 4.30 Access to the OPOLS is only available for Road Agencies, or other licencing authorities as may be agreed by the Coordination Group.
- 4.31 The OPOLS may only be used as part of business processes when processing licence applications, transfers and renewals.
- 4.32 A Road Agency or another licencing authority that accesses the OPOLS must comply with the requirements of the Participation Agreement, including the OPOLS Access Policy developed and maintained by the Coordination Group.
- 4.33 Governance of the OPOLS will be in accordance with the policies and procedures developed and maintained by the Coordination Group in consultation with Road Agencies.

Facial Recognition Analysis Utility Service (FRAUS)

- 4.34 The FRAUS enables each state or territory Road Agency (and any other licencing authority that contributes facial images to the National Driver Licence Facial Recognition Solution) to conduct biometric matching using its own data.

- 4.35 The FRAUS can be used to analyse, de-duplicate and investigate records within each jurisdiction's data holding.
- 4.36 Arrangements for the provision of the FRAUS will be outlined in agreements between the Commonwealth and states and territories relating to the operation of the National Driver Licence Facial Recognition Solution.

Identity Data Sharing Service (IDSS)

- 4.37 The Identity Data Sharing Service (IDSS) enables Agencies to share identity information with another participating Agency in a secure and efficient way. The IDSS does not involve any facial biometric or other data matching.
- 4.38 The IDSS will provide customised functionality that is defined and agreed between agencies that have a lawful basis for sharing identity information and that need to do so on a regular basis.
- 4.39 The Data Holding Agency that owns and controls the identity information will provide, or give permission to provide, the information to a Requesting Agency via the IDSS.
- 4.40 The IDSS will operate in accordance with policies and procedures developed by the Coordination Group.

Part 5 Private Sector Access

Document Verification Service (DVS) Commercial Service

- 5.1 Access to the DVS to match information held by the Commonwealth, states and territories is available to certain Organisations that:
- (a) are required or authorised by a law to require the identification of an individual or to verify the identity of an individual, or
 - (b) have a reasonable need to use government identifiers to verify the identity of an individual.
- 5.2 Private sector access to the DVS is subject to compliance with the DVS Commercial Service Access Policy, including a fee for service arrangement.

Face Verification Service (FVS) Commercial Service

- 5.3 Access to the FVS to match information held by the Commonwealth, states and territories may be made available in the future to certain Organisations that:
- (a) are required or authorised by a law to require the identification of an individual or to verify the identity of an individual, or

- (b) have a reasonable need to use government identifiers and facial images to verify the identity of an individual.

5.4 Private sector access to the FVS to match information held by states and territories will be subject to:

- (a) the express approval of the relevant minister(s) in each state or territory to use their jurisdiction's information for this purpose, to be communicated in writing to the Commonwealth at any stage following signature of this Agreement
- (b) the outcomes of a privacy impact assessment covering the types of Organisations to be given access to the service
- (c) compliance with a FVS Commercial Service Access Policy developed by the Coordination Group, including a fee for service arrangement, and
- (d) an FVS Commercial Service audit and compliance programme overseen by the Coordination Group.

Other Identity Matching Services

5.5 The private sector will not be given access to the other Face Matching Services or the Identity Data Sharing Service.

Part 6 Supporting Systems

6.1 Technical systems have been established to support the operation of the Identity Matching Services by providing the mechanisms for sharing data between Agencies. These systems include:

- (a) the DVS Hub (which does not transmit facial images)
- (b) the interoperability Hub (which supports the Face Matching Services), and
- (c) the National Driver Licence Facial Recognition Solution.

Document Verification Service Hub (DVS Hub)

6.2 The DVS Hub is a technical system or router that securely directs matching requests and responses between user Agencies and Organisations and document issuer Agencies.

6.3 The Commonwealth has established a DVS Hub, and is responsible for its ongoing management and operation, on behalf of the parties.

6.4 The DVS Hub does not retain any identity information once a request or response to a request has been transmitted.

- 6.5 Each party is responsible for the ongoing management and operation of the systems of their respective Agencies that conduct or support DVS verification services.

The interoperability Hub

- 6.6 The interoperability Hub is a technical system that provides a mechanism for the secure and auditable transmission of facial images and related identity information between Agencies and Organisations participating in the Face Matching Services.
- 6.7 The interoperability Hub does not retain any facial images or other identity information; rather it functions as a router to transmit information between participating Agencies and Organisations on a query and response basis.
- 6.8 The Commonwealth is responsible for the ongoing management and operation of the interoperability Hub, on behalf of the parties.
- 6.9 Each party is responsible for any costs associated with integrating their respective Agencies' systems with the interoperability Hub (see Part 10 – Financial Arrangements).
- 6.10 Agencies will initially access the interoperability Hub via a web-based user interface (the Portal) that enables users to log in and manually enter search requests.
- 6.11 Over time, the interoperability Hub will also be able to receive requests via system-to-system connections with Agencies' existing systems.

The National Driver Licence Facial Recognition Solution

- 6.12 As driver licences are currently the most commonly used photographic identity document in Australia, access to these facial images is critical to maximising the benefits provided by the Face Matching Services.
- 6.13 The states and territories agree to participate in the National Driver Licence Facial Recognition Solution as the technical system to enable driver licence facial images and related information to be made available via the Face Matching Services.
- 6.14 The National Driver Licence Facial Recognition Solution is to be hosted by the Commonwealth for the benefit of all parties. The Commonwealth will operate and manage the National Driver Licence Facial Recognition Solution, which will contain identity information contributed by state and territory Data Holding Agencies and the biometric templates generated from that identity information.
- 6.15 The National Driver Licence Facial Recognition Solution comprises:
- (a) a federated database providing each state and territory Road Agency with its own partitioned data store, with individual Agency-based access controls, for facial images and other associated identity information used on driver licences (and

potentially other state and territory government issued evidence documents), replicated from the local system of the document issuing agency

- (b) common facial biometric matching software, managed centrally by the Commonwealth Data Hosting Agency, and
- (c) a central store of biometric templates, derived from facial images replicated by the states and territories using the facial biometric matching software, managed by the Commonwealth Data Hosting Agency.

6.16 The National Driver Licence Facial Recognition Solution:

- (a) will not hold information that is not reasonably necessary to support the Identity Matching Services (such as licence demerit points) which will continue to be held in the local systems of state and territory Road Agencies
- (b) will provide Road Agencies with the FRAUS to undertake analysis, de-duplication and investigation of their own data holdings
- (c) will not provide the Commonwealth Data Hosting Agency with the ability to view, modify or update identity information within each partitioned data store
- (d) will be securely connected to the interoperability Hub to facilitate data sharing with other Agencies via the Face Matching Services, including but not limited to the OPOLS to help determine whether an individual holds multiple driver licences across jurisdictions
- (e) will not provide the Commonwealth with access to identity information within the National Driver Licence Facial Recognition Solution, other than through data sharing arrangements agreed with the relevant state or territory, and
- (f) will not disclose the biometric templates to any other Agency including the Road Agency from whose replicated images the templates were derived.

6.17 The parties acknowledge that:

- (a) identity information held within the National Driver Licence Facial Recognition Solution will be subject to the applicable Commonwealth legislation including the:
 - i. *Freedom of Information Act 1982 (Cth)*, and
 - ii. *Privacy Act 1988 (Cth)*, including the Notifiable Data Breach Scheme in effect from 22 February 2018.
- (b) the Commonwealth will not be required to comply with any state or territory laws or policies as they relate to the identity information while it is held in the National

Driver Licence Facial Recognition Solution, but may agree to abide by equivalent requirements in an agreement with a state or territory Data Holding Agency

- (c) each state and territory is responsible for maintaining the accuracy and integrity of identity information that it replicates to the National Driver Licence Facial Recognition Solution, and
- (d) the Commonwealth will only use or disclose identity information within the National Driver Licence Facial Recognition Solution in accordance with arrangements that are agreed with the relevant state or territory, or where otherwise required by law.

6.18 At the request of a state or territory, other types of facial images (such as images on firearms licences and proof of age cards), may be included in the National Driver Licence Facial Recognition Solution. The inclusion of this information would be subject to:

- (a) the funding arrangements in Part 10 of this Agreement, and
- (b) the relevant state or territory legislation authorising the sharing of this information with the Commonwealth and the use and disclosure of this information by the Commonwealth, in accordance with Part 8 of this Agreement.

6.19 When individuals apply for new or renewed driver licences (or any other documents containing facial images to be used in the National Driver Licence Facial Recognition Solution) Road Agencies (or other relevant licensing agency) will take all reasonable steps to notify these applicants that the personal and sensitive information being collected by the Road Agency may be disclosed for the purposes of biometric matching through the National Driver Licence Facial Recognition Solution for law enforcement, national security and other purposes.

Part 7 Supporting agreements

Document Verification Service

7.1 Cooperative arrangements between the Commonwealth and the states and territories to support the DVS are contained in:

- (a) an agreement between the Commonwealth and Austroads Ltd, as the host of the National Exchange of Vehicle and Driver Information System which holds driver licence information used in the DVS, and
- (b) memoranda of understandings and contracts between Commonwealth Agencies and state and territory Agencies as providers of identity information used in the DVS.

Face Matching Services

7.2 Commonwealth, state and territory Agencies will enter into a common Participation Agreement to provide a legally binding framework within which they will share identity information via the Face Matching Services.

- 7.3 The Participation Agreement will set out the roles, rights and obligations of Data Holding Agencies, Requesting Agencies and the Commonwealth as the operator of the interoperability Hub and Data Hosting Agency for the National Driver Licence Facial Recognition Solution.
- 7.4 The Participation Agreement will provide the framework within which 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.
- 7.5 Arrangements for the operation of the National Driver Licence Facial Recognition Solution will be outlined in agreements between the Commonwealth Agency hosting the National Driver Licence Facial Recognition Solution and the state and territory Road Agencies.
- 7.6 The Participation Agreement and agreements for the National Driver Licence Facial Recognition Solution will be developed and maintained by the Coordination Group.

Part 8 Legislative framework

- 8.1 The parties agree to use their best endeavours to preserve or introduce legislation in each party's respective jurisdiction that enable, with or without further action, the exchange of identity information between Entities participating in the Identity Matching Services.

Legislation to support the DVS

- 8.2 Legislation will be preserved or introduced as appropriate to support the collection, use and disclosure of identity information for the purposes of an Entity's use of the DVS.

Legislation to support the Face Matching Services

- 8.3 Legislation will be preserved or introduced as appropriate to the extent necessary to support the collection, use and disclosure of facial images and related identity information between the parties via the Face Matching Services for the following purposes:
- (a) *Preventing identity crime* — the prevention, detection, investigation or prosecution of identity crime.
 - (b) *General law enforcement* — the prevention, detection, investigation or prosecution of an offence under Commonwealth, or state and/or territory laws.
 - (c) *National security* — conducting investigations or gathering intelligence for purposes relating to Australia's defence, security, international relations or law enforcement interests.

Note: Section 8 of the National Security Information (Criminal and Civil Proceedings) Act 2004 (Cth) defines 'national security' as Australia's defence, security, international relations or law enforcement interests'.

- (d) *Protective security* — activities to promote the security of agency assets, facilities or personnel, including:
 - i. the protection and management of legally assumed identities, and
 - ii. security or criminal background checking.
- (e) *Community safety* — activities to identify individuals who are at risk of, or who have experienced, physical harm, including:
 - i. investigating individuals who are reported as missing
 - ii. identifying individuals who are reported as dead, or unidentified human remains
 - iii. identifying individuals when addressing significant risks to public health or safety, or
 - iv. identifying individuals in relation to disaster events or major events.
- (f) *Road safety*— the conduct of activities to improve road safety, including detection of unlicensed and disqualified drivers and individuals who hold multiple licences.
- (g) *Identity verification* —the verification of an individual’s identity, where this is done with the consent of the individual, for example in the delivery of government services or for private sector organisations to meet regulatory identity verification requirements.

8.4 Clause 8.3 applies to facial images and related identity information used in the following identity documents:

- (a) an Australian passport
- (b) an Australian driver licence
- (c) an ImmiCard or visa issued under the *Migration Act 1958*,
- (d) a certificate of Australian citizenship issued under the *Australian Citizenship Act 2007* (Cth), and
- (e) any other type of identity document with a facial image that a state or territory wishes to include in the National Driver Licence Facial Recognition Solution.

8.5 The legislation preserved or enacted in state and territory jurisdictions should:

- (a) authorise states and territories to provide facial images and related identity information to the host of the National Driver Licence Facial Recognition Solution

- (b) not prohibit the host of the National Driver Licence Facial Recognition Solution from:
 - i. collecting facial images and related identity information
 - ii. using information to enrol facial images into biometric templates and perform biometric facial matching, and
 - iii. disclosing facial images and related identity information to Entities participating in the Face Matching Services.

- (c) authorise, or at the very least not prohibit:
 - i. the exchange of facial images, information and match results via the interoperability Hub
 - ii. the collection of facial images or information from other Agencies via the interoperability Hub, and
 - iii. the disclosure of facial images or information to the interoperability Hub.

8.6 The Commonwealth, as the host of the National Driver Licence Facial Recognition Solution, will ensure it has the necessary legislative authority to host and operate the system.

Part 9 Privacy and protection of personal information

9.1 The parties recognise that the sharing of identity information involves the collection, use and disclosure of personal information, and in the case of the Face Matching Services sensitive personal information, and that the operation of the Identity Matching Services should be subject to robust privacy and security safeguards.

9.2 The Coordination Group will oversee the development, implementation and ongoing operation of multifaceted privacy and security safeguards. This includes the Face Matching Services Participation Agreement and Access Policies which set out the requirements that Agencies and Organisations must meet in order to gain and maintain access to each Face Matching Service.

Security safeguards

9.3 Entities participating in the Face Matching Services will adopt best practice security and access arrangements.

9.4 The Commonwealth will ensure that the interoperability Hub and the National Driver Licence Facial Recognition Solution are subject to independent penetration and vulnerability tests and security reviews.

- 9.5 Access to the Face Identification Service will be restricted to Agencies with law enforcement or national security related functions that are approved by the Coordination Group in accordance with clause 4.19.
- 9.6 Access to the One Person One Licence Service will be limited to specialist fraud prevention or other authorised staff within Road Agencies or other approved licencing authorities.
- 9.7 The Participation Agreement will stipulate any additional security measures required by Data Holding Agencies. Regular audits will help ensure these protections are functioning appropriately.
- 9.8 The Identity Matching Services will be implemented in a manner that ensures the protection of legally assumed and other protected identities. The use of the Identity Matching Services will not contravene a law prohibiting the disclosure of an assumed or protected identity.
- (a) Any face matching services involving 'one-to-many' matching will not commence operation until all parties have confirmed that they are satisfied with the protections for legally assumed identities.

Privacy Safeguards

- 9.9 The Participation Agreement and the Access Policies for each Face Matching Service will outline the privacy safeguards with which Requesting Agencies are required to comply. These include:
- (a) providing a statement of the legislative authority or basis on which the Agency may obtain identity information through the Face Matching Services
- (b) being subject to a privacy impact assessment which includes consideration of the Agency's use of the Face Matching Services, except where the Agency's use of the Face Matching Services is expressly exempt from relevant Commonwealth, state and territory privacy legislation
- (c) entering into arrangements for the sharing of identity information with each Data Holding Agency it wishes to receive information from, within the framework of the Participation Agreement
- (d) providing appropriate training to personnel involved in the use of the Face Matching Services, and
- (e) conducting annual compliance audits, in a manner to be determined by the Coordination Group, in relation to use of the Face Matching Services.
- 9.10 In relation to the arrangements for the sharing of identity information referred to in clause 9.9(c), the Coordination Group will also:
- (a) maintain template arrangements that Agencies may use, and

(b) maintain a publicly available register of such arrangements.

9.11 The FVS Commercial Service Access Policy will contain the privacy safeguards that Organisations must comply with in order to gain and maintain access to the FVS commercial service. The FVS Commercial Service Access Policy will be developed by the Coordination Group.

9.12 The Commonwealth will prepare an annual report on the use of the Identity Matching Services, for the Coordination Group, which includes information such as:

(a) the name of Entities that have accessed, or received information, by using any of the Identity Matching Services, and

(b) the particular services that each Entity has used.

9.13 Agencies and Organisations will also be subject to oversight by the relevant privacy regulator or oversight body within their jurisdiction. This includes the Office of the Australian Information Commissioner for Organisations and Commonwealth Agencies subject to the *Privacy Act 1988* (Cth).

9.14 In addition to complying with the privacy safeguards listed in clause 9.9, Entities must also:

(a) ensure that their collection, use or disclosure of personal information through the Identity Matching Services is reasonable, necessary and proportionate to their functions or activities

(b) only collect, use or disclose personal information through the Identity Matching Services as permitted or required by law, including privacy law, and

(c) maintain accessible and effective mechanisms for responding to any public complaints relating to use of the Identity Matching Services.

Compliance

9.15 If there are concerns about an Entity's compliance with privacy and security safeguards:

(a) the Commonwealth, as the operator of the interoperability Hub, will comply with a direction from a state or territory: to not facilitate; to modify; to suspend; or to terminate an Entity's access to the state or territory's data via the Identity Matching Services, and

(b) the Commonwealth may exercise its discretion: to not facilitate; to modify; to suspend; or to terminate the sharing of information between Entities via the Identity Matching Services.

- i. This discretion should only be exercised after consultation with affected Entities fails to resolve any privacy or security concerns and after consideration of the matter by the Coordination Group.

Note: this may occur, for example, upon receipt of a complaint from a privacy regulator or other oversight body.

- 9.16 Clause 9.15 is not intended to apply to the provision of matching services: within the National Driver Licence Facial Recognition Solution to the Data Holding Agency which contributed that information; or between Agencies within the same state or territory.
- 9.17 The Commonwealth will notify any other affected party of any unauthorised disclosure of the party's identity information via the interoperability Hub or the National Driver Licence Facial Recognition Solution.
- 9.18 Any unauthorised disclosure of identity information via the interoperability Hub or the National Driver Licence Facial Recognition Solution may also, depending on the circumstances of the disclosure, require notification in accordance with the Notifiable Data Breach Scheme established under the Commonwealth *Privacy Act 1988* (Cth).
- 9.19 Arrangements for managing any potential misuse of the Identity Matching Services will be detailed in a Compliance Policy developed and maintained by the Coordination Group.

Training

- 9.20 The parties agree that training users in the appropriate handling of personal and sensitive information obtained via the Face Matching Services is an important privacy safeguard.
- 9.21 Agencies participating in the Face Matching Services will provide appropriate training to personnel involved in the use of these services. This should include:
 - (a) training on how to use the interface and systems of the Face Matching Services
 - (b) privacy and secrecy obligations, and
 - (c) security awareness.
- 9.22 Agencies using the FIS will promote best practice training standards and competencies in personnel undertaking facial recognition and related functions.
- 9.23 Recognising the additional sensitivities associated with access to facial images, a Training Policy for the Face Matching Services will be developed by the Coordination Group to outline suggested minimum mandatory training requirements for users of the Face Matching Services.

Part 10 Financial arrangements

DVS Hub

- 10.1 The Commonwealth is responsible for the ongoing costs of managing and operating the DVS Hub.
- 10.2 Each party is responsible for any other costs associated with the use by their respective participating Agencies of the DVS Hub, including the ongoing costs of managing and operating the systems that conduct or support the DVS.

Interoperability Hub

- 10.3 The Commonwealth is responsible for the ongoing costs of managing and operating the interoperability Hub, including a generic web-based user interface for Agencies.
- 10.4 Each party will be responsible for any other costs associated with the use by their respective Agencies (both Requesting Agencies and Data Holding Agencies) of the Interoperability Hub, including:
- (a) the operating costs of their Agencies' internal systems
 - (b) costs associated with connecting to the Interoperability Hub
 - (c) costs associated with developing a system-to-system connection if requested by an Agency of the party, and
 - (d) Agency-specific customisations of the user interface.

National Driver Licence Facial Recognition Solution

- 10.5 The estimated cost of establishing and operating the central technical infrastructure of the National Driver Licence Facial Recognition Solution is \$21 million over four years from 2016-17 to 2019-20. This includes \$14 million in initial establishment costs (including the costs of a technical solution for protecting legally assumed identities).
- 10.6 The Commonwealth will meet the establishment costs for central technical infrastructure of the National Driver Licence Facial Recognition Solution.
- 10.7 Annual operating and maintenance costs, initially of approximately \$2.3 million per year, will be shared. The Commonwealth will fund 50 percent of these costs. The other 50 percent will be shared by the states and territories, on a population basis. The funding contributions for each state and territory are outlined in Schedules to this Agreement.
- 10.8 These contributions will enable the National Driver Licence Facial Recognition Solution to hold the current driver licence images from all states and territories.
- 10.9 The cost of including any additional images will be subject to negotiation between the Commonwealth and the relevant state or territory.

- (a) Unless otherwise agreed by the Commonwealth, the costs associated with including these facial images will be met by the party requesting their inclusion in the system.

10.10 The annual funding contributions sought from each state and territory will not increase if one or more jurisdictions decide not to participate in the National Driver Licence Facial Recognition Solution, or delays a decision to participate.

10.11 The contributions sought from each state and territory towards the operation and maintenance of the National Driver Licence Facial Recognition Solution will be re-assessed annually by the Coordination Group.

10.12 A broader review of financial arrangements will be conducted by the Coordination Group, one year after all jurisdictions are participating in the Face Matching Services, or within two years of the commencement of this Agreement, whichever is sooner.

10.13 Each party will be responsible for any other costs associated with the participation of their respective Road Agencies in the National Driver Licence Facial Recognition Solution, including:

- (a) the costs of their Road Agencies' internal systems
- (b) upgrading their Road Agencies' systems to enable connection with the National Driver Licence Facial Recognition Solution to provide and receive information through the Face Matching Services
- (c) upgrading processes and procedures for maintaining high quality data, including the capture of facial images suitable for facial biometric matching, and
- (d) upgrading police or other Agency systems to use the National Driver Licence Facial Recognition Solution.

Privacy oversight

10.14 Each party will be responsible for any additional resourcing of privacy regulators and other oversight bodies that may be required to ensure the compliance of their respective Agencies with this Agreement.

General provisions on funding

10.15 There is nothing in this Agreement that prohibits any party from introducing fees or charges for the provision of the Identity Matching Services between the parties, or between the parties and Organisations, provided that any such fees or charges are developed and implemented in accordance with the Charging Policy to be developed and maintained by the Coordination Group.

10.16 Where a party is obliged to make a financial contribution or other payment under this Agreement, that contribution or payment must be made in a timely fashion and in accordance with procedures developed and agreed by the Coordination Group.

10.17 To clarify:

- (a) a party may enter into any other financial commitments with another party, and
- (b) nothing in this Agreement is intended to qualify or affect the rights of any of the parties to make decisions about the expenditure or commitment of their own funding.

Part 11 Governance and accountability

Ministerial oversight

- 11.1 The Ministerial Council for Police and Emergency Management (MCPEM) will exercise ministerial oversight of the Identity Matching Services.
- 11.2 The MCPEM will consult with the Transport and Infrastructure Council (TIC), as required, on matters relating to the participation of Road Agencies in the Identity Matching Services, including on the National Driver Licence Facial Recognition Solution.
- 11.3 The MCPEM will have responsibility for considering significant new policy matters in relation to the Identity Matching Services.
- 11.4 Any consideration of significant new policy matters should include a consideration of its impact on privacy and the public interest.
- 11.5 The MCPEM will also have responsibility for approving the Terms of Reference for the Coordination Group, as the body to be responsible to MCPEM for the management of the Identity Matching Services.

National Identity Security Coordination Group (Coordination Group)

- 11.6 The Coordination Group is accountable to the MCPEM for the efficient and effective delivery and management of the Identity Matching Services.

Note: The Coordination Group was first established under the Intergovernmental Agreement to a National Identity Security Strategy, agreed to by the Council of Australian Governments on 13 April 2007.

- 11.7 The Coordination Group's responsibilities and functions in relation to the management of the Identity Matching Services include:
 - (a) overseeing implementation of technical solutions to support the operation of the Identity Matching Services
 - (b) overseeing the development and implementation of robust data access controls, security and privacy regimes, including:
 - i. policy and contractual terms for government and private sector users of the DVS

- ii. policy and model data sharing agreements for Agencies participating in the face matching services, and
- iii. training materials to promote best practice use of the Identity Matching Services by participating Agencies and Organisations
- (c) overseeing the operation of audit, compliance and assurance activities to ensure the continued effectiveness of privacy and security safeguards, including:
 - i. reviewing actions undertaken in response to audit and compliance reports from participating Agencies, and
 - ii. considering matters referred to the Coordination Group for decision, including recommendations for suspension or termination of an Organisation's access to the Identity Matching Services
- (d) managing risks associated with the operation of the Identity Matching Services
- (e) considering proposals for:
 - i. improving the national operation of the Identity Matching Services, or
 - ii. new national initiatives to enhance and expand the Identity Matching Servicesand, where approved, coordinating their timely implementation across jurisdictions
- (f) advising governments on the financial investments and arrangements needed to support the ongoing operation of the Identity Matching Services
- (g) providing a central point of coordination for consultation with jurisdictional stakeholders
- (h) reporting annually to the MCP EM on the operation of the Identity Matching Services, and
- (i) coordinating a review of the operation of the Identity Matching Services every three years.

11.8 The Coordination Group will have membership drawn from:

- (a) the Commonwealth Attorney-General's Department or other lead Commonwealth Agency, to act as the chair, and
- (b) each state and territory first minister's department, or other lead Agency.

11.9 The Coordination Group will also include representation, as observers, from:

- (a) the Office of the Australian Information Commissioner

- (b) the National Criminal Intelligence Capability Committee of the Australian Criminal Intelligence Commission as a sworn police officer representing state and territory police Agencies, and
- (c) Austroads as a representative of Road Agencies.

11.10 The Coordination Group may establish advisory committees and working groups as needed, including a steering committee for the National Driver Licence Facial Recognition Solution.

11.11 The clauses in this Agreement operate in addition to clause 10 (governance arrangements of the National Identity Security Coordination Group) of the *Intergovernmental Agreement to a National Identity Security Strategy*, agreed to by the Council of Australian Governments on 13 April 2007. The clauses in this Agreement prevail where there is any inconsistency between this Agreement and clause 10 of the 2007 Agreement.

Part 12 General

Commencement

- 12.1 This Agreement will commence when at least one Schedule to this Agreement has been co-signed by the Commonwealth and the relevant state or territory.
- 12.2 This Agreement will be effective between any parties that have signed a Schedule to this Agreement from the date of the parties' signature.
- 12.3 Upon signature of the relevant Schedule, a party agrees to both the content in this Agreement and the relevant Schedule to this Agreement, subject to any variations to this Agreement as outlined in the relevant Schedule.
- 12.4 Upon signature of the relevant Schedule, parties agree to share identity information, subject to their jurisdictional legal framework, through the Identity Matching Services with all other parties that sign a Schedule to this Agreement, noting that each Data Holding Agency retains discretion over which Agencies it will share data with, to be exercised through the Participation Agreement.

Enforceability

- 12.5 The Schedules to this Agreement form part of this Agreement once signed by the Commonwealth and relevant jurisdictions.
- 12.6 The parties do not intend any of the provisions of this Agreement to be legally enforceable. However, that does not lessen the parties' commitment to this Agreement.
- 12.7 When signing this Agreement, states and territories may specify that a variation be made to an existing provision, or new a provision be added to this Agreement, that relates solely to that jurisdiction and/or the Commonwealth's interaction with that jurisdiction. These will be contained in relevant Schedules to this Agreement.

Nothing to affect existing rights, obligations or agreements

- 12.8 Nothing in this Agreement affects or limits a party's existing rights, obligations, laws or other agreements, including in relation to privacy or information sharing.
- 12.9 This Agreement operates in parallel with, and does not override, the *Intergovernmental Agreement to a National Identity Security Strategy*, agreed to by the Council of Australian Governments on 13 April 2007, except for clause 11.11 which specifies that this Agreement prevails where there is any inconsistency.

Dispute resolution

- 12.10 Any party may give written notice to other parties of a dispute under this Agreement.
- 12.11 Officials of relevant parties will attempt in good faith to resolve any dispute in the first instance.
- 12.12 If a dispute is unable to be resolved by officials, it may be escalated to the relevant Ministers and if necessary, MCPPEM.

Variation, withdrawal and termination

- 12.13 The Schedules to the Agreement provide the means for jurisdictions to vary particular aspects of this Agreement.
- 12.14 The Schedules to this Agreement may be amended at any time by agreement in writing between the relevant Commonwealth and the relevant state or territory ministers. Notification of any suggested changes will be provided to all other signatories to the Agreement.
- 12.15 This Agreement may be amended at any time by agreement in writing by MCPPEM, except for the Schedules to the Agreement which may be amended in accordance with clause 12.14.
- 12.16 A party may withdraw from the Agreement at any time by notifying all other parties in writing and giving not less than three months' notice.
- 12.17 If a state or territory withdraws from this Agreement, the facial images and other identity information that its Agencies have contributed to the National Driver Licence Facial Recognition Solution, together with the associated biometric templates, will be removed as soon as practicable.
- 12.18 A party may not withdraw from this Agreement if it has not met its financial commitments under Part 10 (Financial arrangements), unless that party's withdrawal, and the terms of its withdrawal, is agreed to by all other parties.
- 12.19 Upon a party's withdrawal from this Agreement, that party will have no right to claim compensation or payment in respect of any assets, including intellectual property rights or

monies which it has contributed under this Agreement. That party's participating Agencies may also lose their ability to access the Identity Matching Services.

12.20 If a party withdraws from this Agreement, this Agreement will remain in force in relation to the remaining parties.

12.21 This Agreement may be terminated at any time by agreement in writing by all parties and under any terms and conditions as agreed by all parties.

Part 13 Review

13.1 In accordance with clause 4.25 above, the Coordination Group will review the definition and operation of the general law enforcement purpose one year after the commencement of the FIS and report the outcomes of the review to the MCPPEM.

13.2 In accordance with clause 10.12 above, the Coordination Group will conduct a review of financial arrangements for the Face Matching Services one year after all jurisdictions are participating in one or more of the Face Matching Services, or within two years of the commencement of this Agreement, whichever is sooner.

13.3 The operation of the Identity Matching Services more broadly will be reviewed three years from the commencement of this Agreement to assess matters including but not limited to:

- (a) effectiveness in progressing the objective of this Agreement
- (b) effectiveness of governance arrangements, and
- (c) privacy impact and effectiveness of privacy safeguards in protecting the personal information of individuals.

13.4 The review will be provided to the MCPPEM as the ministerial level governing body for the Identity Matching Services.

13.5 The terms of reference for the review will be determined by the Coordination Group.

13.6 The review will be published online by the Commonwealth.

SCHEDULE A – NEW SOUTH WALES

This Schedule sets out New South Wales' financial contributions towards the National Driver Licence Facial Recognition Solution.

New South Wales' financial contribution to the National Driver Licence Facial Recognition Solution

A.1 In accordance with the funding arrangements set out in clauses 10.5 – 10.13 of the Agreement, New South Wales will provide the Commonwealth with \$364,000 per year from 2018-19 towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.

A.2 This contribution will help support ongoing access to identity information within the National Driver Licence Facial Recognition Solution, via the Face Matching Services, for the following agencies:

1. Roads and Maritime Service, New South Wales
2. New South Wales Police Force
3. New South Wales Crime Commission
4. New South Wales Independent Commission Against Corruption (ICAC), and
5. New South Wales Law Enforcement Conduct Commission.

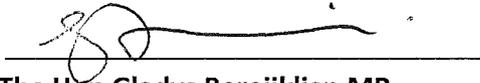
A.3 The provision of access to additional New South Wales Government agencies may be subject to further costs.

A.4 This contribution may be varied via an agreement between the Commonwealth Attorney-General's Department and participating New South Wales Government agencies, following a review of funding arrangements for the National Driver Licence Facial Recognition Solution.

A.5 Any costs associated with integrating the systems of the New South Wales road agency with the National Driver Licence Facial Recognition Solution are the responsibility of New South Wales.

New South Wales confirms their commitment to this Agreement:

Signed for and on behalf of New South Wales by



The Hon Gladys Berejiklian MP

Premier of New South Wales

Date

The Commonwealth confirms their commitment to this Agreement:

Signed for and on behalf of the Commonwealth by



The Hon Malcolm Turnbull MP

Prime Minister of Australia

Date

SCHEDULE B – VICTORIA

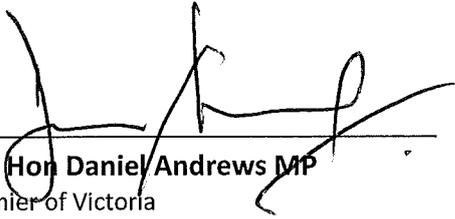
This Schedule sets out Victoria's financial contributions towards the National Driver Licence Facial Recognition Solution.

Victoria's financial contribution to the National Driver Licence Facial Recognition Solution

- A.1 In accordance with the funding arrangements set out in clauses 10.5 – 10.13 of the Agreement, Victoria will provide the Commonwealth with \$264,000 per year from 2018-19 towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.
- A.2 This contribution will help support ongoing access to identity information within the National Driver Licence Facial Recognition Solution, via the Face Matching Services, for the following agencies:
1. Roads Corporation Victoria
 2. Victoria Police, and
 3. Independent Broad-Based Anti-Corruption Commission.
- A.3 The provision of access to additional Victorian Government agencies may be subject to further costs.
- A.4 This contribution may be varied via an agreement between the Commonwealth Attorney-General's Department and participating Victorian Government agencies, following a review of funding arrangements for the National Driver Licence Facial Recognition Solution.
- A.5 Any costs associated with integrating the systems of the Victorian road agency with the National Driver Licence Facial Recognition Solution are the responsibility of Victoria.

Victoria confirms their commitment to this Agreement:

Signed for and on behalf of Victoria by



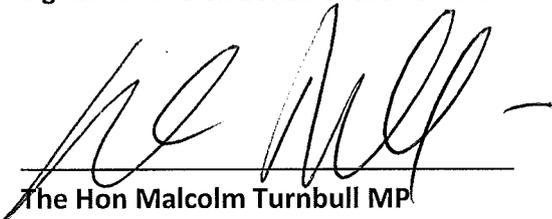
A handwritten signature in black ink, appearing to read 'Daniel Andrews', is written over a horizontal line.

The Hon Daniel Andrews MP
Premier of Victoria

Date

The Commonwealth confirms their commitment to this Agreement:

Signed for and on behalf of the Commonwealth by



A handwritten signature in black ink, appearing to read 'Malcolm Turnbull', is written over a horizontal line.

The Hon Malcolm Turnbull MP
Prime Minister of Australia

Date

SCHEDULE C – QUEENSLAND

This Schedule sets out Queensland’s financial contributions towards the National Driver Licence Facial Recognition Solution.

Queensland’s financial contribution to the National Driver Licence Facial Recognition Solution

A.1 In accordance with the funding arrangements set out in clauses 10.5 – 10.13 of the Agreement, Queensland will provide the Commonwealth with \$202,000 per year from 2018-19 towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.

A.2 This contribution will help support ongoing access to identity information within the National Driver Licence Facial Recognition Solution, via the Face Matching Services, for the following agencies:

1. Department of Transport and Main Roads
2. Queensland Police Service, and
3. Crime and Corruption Commission.

A.3 The provision of access to additional Queensland Government agencies may be subject to further costs.

A.4 This contribution may be varied via an agreement between the Commonwealth Attorney-General’s Department and participating Queensland Government agencies, following a review of funding arrangements for the National Driver Licence Facial Recognition Solution.

A.5 Any costs associated with integrating the systems of the Queensland road agency with the National Driver Licence Facial Recognition Solution are the responsibility of Queensland.

Queensland confirms their commitment to this Agreement:

Signed for and on behalf of Queensland by



The Hon Anastacia Palaszczuk MP

Premier of Queensland

Date

The Commonwealth confirms their commitment to this Agreement:

Signed for and on behalf of the Commonwealth by



The Hon Malcolm Turnbull MP

Prime Minister of Australia

Date

SCHEDULE D – WESTERN AUSTRALIA

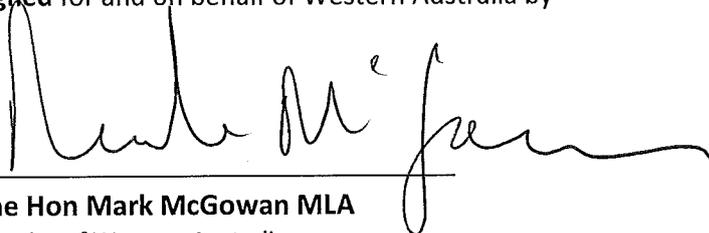
This Schedule sets out Western Australia’s financial contributions towards the National Driver Licence Facial Recognition Solution.

Western Australia’s financial contribution to the National Driver Licence Facial Recognition Solution

- A.1 In accordance with the funding arrangements set out in clauses 10.5 – 10.13 of the Agreement, Western Australia will provide the Commonwealth with \$122,000 per year from 2018-19 towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.
- A.2 This contribution will help support ongoing access to identity information within the National Driver Licence Facial Recognition Solution, via the Face Matching Services, for the following agencies:
1. Department of Transport
 2. Western Australia Police Force, and
 3. Corruption and Crime Commission.
- A.3 The provision of access to additional Western Australian Government agencies may be subject to further costs.
- A.4 This contribution may be varied via an agreement between the Commonwealth Attorney-General’s Department and participating Western Australian Government agencies, following a review of funding arrangements for the National Driver Licence Facial Recognition Solution.
- A.5 Any costs associated with integrating the systems of the Western Australian road agency with the National Driver Licence Facial Recognition Solution are the responsibility of Western Australia.

Western Australia confirms their commitment to this Agreement:

Signed for and on behalf of Western Australia by

A handwritten signature in black ink, appearing to read 'Mark McGowan', written over a horizontal line.

The Hon Mark McGowan MLA
Premier of Western Australia

Date

The Commonwealth confirms their commitment to this Agreement:

Signed for and on behalf of the Commonwealth by

A handwritten signature in black ink, appearing to read 'Malcolm Turnbull', written over a horizontal line.

The Hon Malcolm Turnbull MP
Prime Minister of Australia

Date

SCHEDULE E – SOUTH AUSTRALIA

This Schedule sets out:

- (a) South Australia's financial contributions towards the National Driver Licence Facial Recognition Solution, and
- (b) variations to this Agreement, specific to South Australia's participation in the Identity Matching Services.

South Australia's financial contribution to the National Driver Licence Facial Recognition Solution

A.1 In accordance with the funding arrangements set out in clauses 10.5 – 10.13 of the Agreement, South Australia will provide the Commonwealth with \$79,000 per year from 2018-19 towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.

A.2 This contribution will help support ongoing access to identity information within the National Driver Licence Facial Recognition Solution, via the Face Matching Services, for the following agencies:

1. Department of Planning, Transport and Infrastructure
2. South Australia Police
3. Independent Commissioner Against Corruption, and
4. Office for Public Integrity.

A.3 The provision of access to additional South Australian Government agencies may be subject to further costs.

A.4 This contribution may be varied via an agreement between the Commonwealth Attorney-General's Department and participating South Australian Government agencies, following a review of funding arrangements for the National Driver Licence Facial Recognition Solution.

A.5 Any costs associated with integrating the systems of the South Australian road agency with the National Driver Licence Facial Recognition Solution are the responsibility of South Australia.

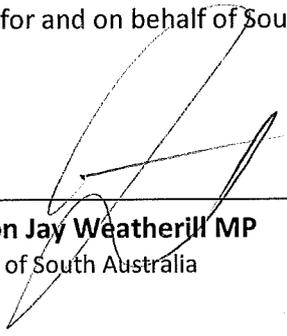
Variations to this Agreement specific to South Australia

A.6 South Australia's acceptance of this Agreement is provided on the basis of variations to the clauses of the Agreement as follows:

The *Public Sector (Data Sharing) Act 2016* will provide authorisation for the purposes of clause 8.5 of the Agreement.

South Australia confirms their commitment to this Agreement:

Signed for and on behalf of South Australia by



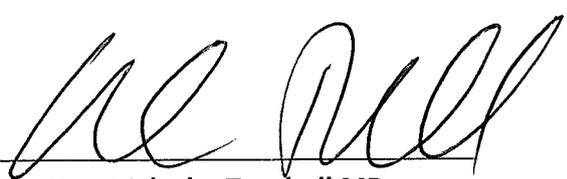
The Hon Jay Weatherill MP

Premier of South Australia

Date

The Commonwealth confirms their commitment to this Agreement:

Signed for and on behalf of the Commonwealth by



The Hon Malcolm Turnbull MP

Prime Minister of Australia

Date

SCHEDULE F – TASMANIA

This Schedule sets out Tasmania’s financial contributions towards the National Driver Licence Facial Recognition Solution.

Tasmania’s financial contribution to the National Driver Licence Facial Recognition Solution

A.1 In accordance with the funding arrangements set out in clauses 10.5 – 10.13 of the Agreement, Tasmania will provide the Commonwealth with \$30,000 per year from 2018-19 towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.

A.2 This contribution will help support ongoing access to identity information within the National Driver Licence Facial Recognition Solution, via the Face Matching Services, for the following agencies:

1. Department of State Growth
2. Tasmania Police, and
3. Integrity Commission.

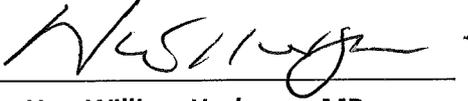
A.3 The provision of access to additional Tasmanian Government agencies may be subject to further costs.

A.4 This contribution may be varied via an agreement between the Commonwealth Attorney-General’s Department and participating Tasmanian Government agencies, following a review of funding arrangements for the National Driver Licence Facial Recognition Solution.

A.5 Any costs associated with integrating the systems of the Tasmanian road agency with the National Driver Licence Facial Recognition Solution are the responsibility of Tasmania.

Tasmania confirms their commitment to this Agreement:

Signed for and on behalf of Tasmania by



The Hon William Hodgman MP
Premier of Tasmania

Date

The Commonwealth confirms their commitment to this Agreement:

Signed for and on behalf of the Commonwealth by



The Hon Malcolm Turnbull MP
Prime Minister of Australia

Date

SCHEDULE G – AUSTRALIAN CAPITAL TERRITORY

This Schedule sets out:

- (c) the Australian Capital Territory’s financial contributions towards the National Driver Licence Facial Recognition Solution, and
- (d) variations to this Agreement, specific to the Australian Capital Territory’s participation in the Identity Matching Services.

Australian Capital Territory’s financial contribution to the National Driver Licence Facial Recognition Solution

A.6 In accordance with the funding arrangements set out in clauses 10.5 – 10.13 of the Agreement, the Australian Capital Territory will provide the Commonwealth with \$20,000 per year from 2018-19 towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.

A.7 This contribution will help support ongoing access to identity information within the National Driver Licence Facial Recognition Solution, via the Face Matching Services, for the following agencies:

1. Access Canberra, and
2. ACT Policing.

A.8 The provision of access to additional Australian Capital Territory Government agencies may be subject to further costs.

A.9 This contribution may be varied via an agreement between the Commonwealth Attorney-General’s Department and participating Australian Capital Territory Government agencies, following a review of funding arrangements for the National Driver Licence Facial Recognition Solution.

A.10 Any costs associated with integrating the systems of the Australian Capital Territory road agency with the National Driver Licence Facial Recognition Solution are the responsibility of the Australian Capital Territory.

Variations to this Agreement specific to the Australian Capital Territory

A.11 The Australian Capital Territory's agreement to participate in the Face Matching Services is provided on the basis that:

- a. The Australian Capital Territory:
 - i. will allow access to its data via the Face Verification Service for the purposes listed in clause 1.2;
 - ii. will allow access to its data via the Face Identification Service for the purposes of national security and community safety only;
 - iii. will not participate in the One Person One Licence System at this stage.
- b. The Australian Capital Territory only agrees to participate in the Face Matching Services to the extent agreed to through the Face Matching Services Participation Agreement. The ACT will legislate as appropriate to give effect to the commitments contained in that Participation Agreement.
- c. The Australian Capital Territory notes the importance of human rights, specifically the right to privacy. Any participation in the Capability by the Australian Capital Territory will be consistent with the human rights principles as set out in the *Human Rights Act 2004* (ACT).

The Australian Capital Territory confirms their commitment to this Agreement:

Signed for and on behalf of the Australian Capital Territory by



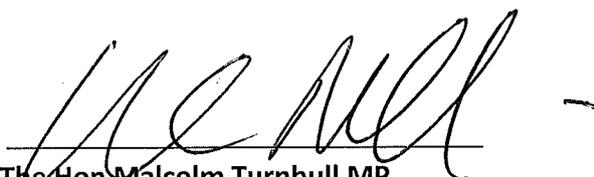
Andrew Barr MLA

Chief Minister of the Australian Capital Territory

Date

The Commonwealth confirms their commitment to this Agreement:

Signed for and on behalf of the Commonwealth by



The Hon Malcolm Turnbull MP

Prime Minister of Australia

Date

SCHEDULE H – NORTHERN TERRITORY

This Schedule sets out the Northern Territory's financial contributions towards the National Driver Licence Facial Recognition Solution.

Northern Territory's financial contribution to the National Driver Licence Facial Recognition Solution

- A.1 In accordance with the funding arrangements set out in clauses 10.5 – 10.13 of the Agreement, Northern Territory will provide the Commonwealth with \$14,700 per year from 2018-19 towards the ongoing operating and maintenance costs of the National Driver Licence Facial Recognition Solution.
- A.2 This contribution will help support ongoing access to identity information within the National Driver Licence Facial Recognition Solution, via the Face Matching Services, for the following agencies:
1. Department of Infrastructure, Planning and Logistics, and
 2. Northern Territory Police.
- A.3 The provision of access to additional Northern Territory Government agencies may be subject to further costs.
- A.4 This contribution may be varied via an agreement between the Commonwealth Attorney-General's Department and participating Northern Territory Government agencies, following a review of funding arrangements for the National Driver Licence Facial Recognition Solution.
- A.5 Any costs associated with integrating the systems of the Northern Territory road agency with the National Driver Licence Facial Recognition Solution are the responsibility of the Northern Territory.

Northern Territory confirms their commitment to this Agreement:

Signed for and on behalf of the Northern Territory by



The Hon Michael Gunner MLA
Chief Minister of the Northern Territory

Date

The Commonwealth confirms their commitment to this Agreement:

Signed for and on behalf of the Commonwealth by



The Hon Malcolm Turnbull MP
Prime Minister of Australia

Date