Austroads

Austroads' response to the Australian Government's Digital Identity Legislation (Phase 3: TDI Bill)

Contents

1. Introduction

Austroads Limited (**Austroads**) is a not-for-profit member-based organisation that comprises of and represents, among others, each of the eight Australian state and territory transport agencies.

Austroads welcomes the Australian Government's consultation on the exposure draft of the *Trusted Digital Identity TDI Bill 2021* released on 1 October 2021 (the **TDI Bill**). We note this is the third phase of the Digital Transformation Agency's (**DTA**) public consultation on the Trusted Digital Identity legislation.

We note that the majority of the positions outlined in Digital Identity Legislation Position Paper which was released on 10 June 2021 (**Position Paper**) remain unchanged and are reflected in the TDI Bill. As such, the issues set out below largely reflect the feedback Austroads and its members have previously provided to the DTA.

Austroads is pleased to make this submission and to suggest ways Austroads and its members can support the delivery of the Commonwealth's Trusted Digital Identity System (or **System**). Our submission covers:

- **Part 1:** the role of Austroads in national identity reform and other identity initiatives;
- **Part 2:** specific comments on the TDI Bill and associated rules including the areas where Austroads' members require greater clarity; and
- **Part 3:** general observations on how the experience and expertise of the state and territory road and transport agencies in developing workable and practical identity verification architecture and processes may be more effectively leveraged to ensure the success of the System.

Austroads understands there is a limited time period between the close of the consultation period (being 27 October) and the intended tabling of the TDI Bill in Federal Parliament. This means it will be difficult for issues raised in this phase of the consultation to be addressed by the DTA before the end of the year. However Austroads would like the Commonwealth Government to take the views in this submission into account as amendments, prior to introduction to Parliament, or as the TDI Bill progresses through the two chambers, either in the Consideration in Detail phase, or when being considered by the Senate Standing Committee for the Scrutiny of Bills or other Parliamentary committees. We expect that the submissions received in this phase of the consultation process will prompt a number of amendments which will ensure greater alignment with the key objects of the TDI Bill to:

- provide individuals with a simple and convenient method for verifying their identity in online transactions with government and businesses, while protecting their privacy and the security of their personal (including biometric) information; and
- facilitate economic benefits and encourage innovation by using digital identities, online services and the interoperability of systems.

2. Austroads' role in national identity reform

Austroads and its members have worked with Commonwealth justice agencies over the last 30 years to develop architecture and processes which support the secure verification/validation of identities and related attributes that are appropriate for the federation.

Since its establishment in 1998, Austroads has hosted the National Exchange of Vehicle and Driver Information System (**NEVDIS**) on behalf of the eight states and territory jurisdictions who contribute their registration and licensing data. NEVDIS is a single consistent national repository of registration and driver licensing information that is owned and managed by Austroads. NEVDIS has been integrated with the Document Verification Service (DVS) since 2009 to support agencies and other authorised users to electronically verify evidence of identity documents and make identity-based decisions. DVS uses NEVDIS identities to establish online accounts like MyGovID.

Austroads has invested heavily in the technology that supports NEVDIS and its interface with the DVS. Further detail on the development and use of NEVDIS is set out in ***Appendix A***.

As the entity responsible for managing NEVDIS, Austroads has been central to a range of other initiatives since the early 2000s aimed at developing nationally consistent approaches to identity verification. Further detail on how Austroads has supported national identity reform is set out in ***Appendix B***.

2.1 NEVDIS and national identity architecture

NEVDIS operates within the broader identity verification ecosystem, which includes the DVS and, subject to the passage of legislation, the Facial Verification System (**FVS**). Though they will be regulated by the *Identity Matching Services TDI Bill 2019 (Cth)* (**IMS Bill**) rather than the TDI Bill, the DVS and FVS will be key inputs into the System as the primary tools that will be used by accredited identify service providers to verify the attributes of a user who creates a digital identity in the System.

The DVS is currently owned by and, through the National Identity Security Coordination Group and its supporting DVS Advisory Board, operated by the state, territory and federal governments. The DVS system uses an electronic gateway known as the DVS Hub to securely direct requests and responses between approved DVS user entities and issuer agencies. Austroads acts as an "issuer agency" on behalf of each of the transport agencies and responds to verification requests from authorised users seeking to check biographic information against licence data held on NEVDIS. These interactions occur outside of the System and are therefore not covered by the TDI Bill.

The FVS will be used to verify driver licence biometrics once the IMS Bill is passed. States and territories will provide facial images on drivers' licences direct to the National Driver Licence Facial Recognition Solution (NDLFRS), a database hosted by the Commonwealth. As with the DVS, verification of an individual's facial features for the purposes of creating a Digital Identity against the FVS (for example, using selfie software) is not covered by the TDI Bill.

2.2 Austroads' members well positioned to help government achieve the TDI Bill's objects

Austroads' members have statutory functions and responsibilities in relation to the issuing of driver licences and the collection and management of associated licence data for the purposes of authorised road use in various forms. Licences have also become a core de facto and essential primary identity document for the community and, are most relied on by individuals as a primary means of verifying identity using documentary and biometric credentials. As data custodians, Austroads' members are responsible for the integrity and reliability of licence data and also have a critical role in its ongoing protection. The driver licence is also considered a proof of identity in a number of regulatory and policy settings outside transport authorities and Austroads members have experience in understanding the legislative and policy impacts of identity acceptance in the community.

In collaboration with service delivery and law enforcement agencies, Austroads' members also have significant service digitisation experience including in connection with the development and implementation of state-based verification and authentication frameworks. Austroads' members therefore are experienced in providing access to state and territory services through online channels and understand the concerns and expectations of their constituents when interacting digitally with government. These constituents are likely to be a significant segment of the System's potential userbase, meaning the insights and lessons learned to date will be critical to inform the development of the System and the protection of covered information. Austroads believes that this experience and capability can and should continue to be leveraged by the Commonwealth to help inform the continued development and design of the System and related identity services as well as its digital transformation strategy more broadly. This includes co-design of the Bill and the further development of associated rules[1] and technical standards that will support the System and its interoperability. These include policy, architecture, governance, operating model, NEVDIS data use and protection, as well as the charging framework.

[1] The TDI Bill allows the Minister to make additional operationally focussed rules which are legally binding. The rules will be "disallowable instruments" meaning they must be tabled in Parliament and can be disallowed.

3. Comments on specific aspects of the TDI Bill

Austroads acknowledges and thanks the DTA for its work to date to establish a trusted federal and interoperable digital identity system for Australia and a robust accreditation process to support it. The System, once implemented on a whole-of-economy basis, will facilitate a coordinated approach to standards and design to achieve national consistency in the delivery of digital identity services with a focus on consumers.

However, Austroads and its members have feedback on various aspects of the TDI Bill. The key issues impacting our members' ability to make informed decisions about how they will participate in the System are outlined below. We note that the majority of the positions outlined in Digital Identity Legislation Position Paper which released on 10 June 2021 (**Position Paper**) remain unchanged and are reflected in the TDI Bill. As such, the issues set out below largely reflect the feedback Austroads and its members have previously provided to the DTA.

3.1 Costs of participation

The TDI Bill authorises the Australian Government to make rules (to be set out in subordinate legislation, namely the TDI Rules) related to charging for the System by the Oversight Authority and by accredited entities.[2] The relevant rules remain under development and the DTA has confirmed in materials accompanying the release of the TDI Bill that these rules will be subject to further consultation, which Austroads welcomes.

However, Austroads understands that the relevant charging framework is unlikely to be released for public comment prior to the TDI Bill being tabled in Parliament. The justification for this, as set out in the Position Paper, was to allow for "a comprehensive stakeholder consultation process for the charging framework and the collection of data as the system is rolled out beyond the Australian Government".[3] However as noted in Austroads' previous submission, the current lack of clarity about the costs of participation as the TDI Bill is introduced, is an ongoing concern. For example, the proposed charging principles may expose our members to charges for accessing their own data (driver licence data) as a relying party to verify the identity of an individual seeking access to an online state service.

In addition to the fees associated with use of the System, state and territory government agencies may incur costs transitioning from or decommissioning existing digital identity solutions, as well as updating existing legislation, regulations and policies, to ensure alignment with the new regulatory scheme.[4]

Without further detail on how state and territory participation in the System could be incentivised under the charging framework, it will be challenging for our members to make informed and meaningful decisions about accreditation and participation in the System. Our members query why the jurisdictions should be required to pay for a federally supported service where significant investment has been made in state-based digital identification solutions which offer equivalent outcomes and are operational at no additional cost. Austroads therefore seeks further clarity and consultation on the proposed charging framework and to understand when this will happen.

[2] See Chapter 7, Part 5, *TDI Bill*
[3] See section 11, *Position Paper*
[4] This position is reflected in the *Consultation Regulation Impact Statement*, see section 9.1.3.

3.2 Oversight Authority and cross-jurisdictional representation

Consistent with the Position Paper, the TDI Bill establishes the Oversight Authority. We note the Oversight Authority is a statutory office held by an individual, more akin to other statutory officers, such as the Director-General of Security or the Commissioner of Taxation, rather than a statutory authority, such as the Productivity Commission or the Australian Securities and Investment Commission.

The office holder of the Oversight Authority is responsible for governing the System and the Trusted Digital Identity Framework (**TDIF**) accreditation scheme.[5] The Information Commissioner has also been granted additional privacy-related regulatory functions under the TDI Bill.[6]

While the TDI Bill does not specify which existing Commonwealth Department will house or support the Oversight Authority, it does make clear that supporting staff will be drawn from an existing Commonwealth department.[7] This creates a risk that there may be a lack of oversight independence by the Oversight Authority and its supporting staff, which may impact their approach to breaches and instances of non-compliance that are critical to maintaining trust in the System.

As the custodians of the most commonly used photographic identity document in Australia at this time, our members are concerned about the lack of state and territory or cross-jurisdictional representation in the proposed governance arrangements. Current arrangements limit the ability of the state and territory transport agencies to protect the integrity and reliability of the driver licence data used to create a Digital Identity in line with their statutory responsibilities and broader community expectations. For example, where the occurrence of a security or fraud incident in the System compromises driver licence data (or, alternatively, occurs from the use of a stolen or compromised licence in the first instance), our members will have limited (if any) visibility over response and remediation activities, as well as ongoing efforts to ensure compliance with relevant legislation. This is because under the TDI Bill assisting victims of identity fraud or a security incident, promoting compliance with the TDI Bill and approving or suspending the onboarding of entities are functions of the Oversight Authority and no mechanism has been provided for jurisdictional input or oversight of the exercise of these functions.

Austroads understands that state and territory representatives have sought to collectively engage with the DTA on governance arrangements and proposed options for enabling meaningful jurisdictional input and oversight. Ostensibly, the Oversight Authority will have interjurisdictional responsibilities or shared functions. This is reflected in the establishment of the Digital Identity Cross-jurisdictional Working Group (DICJWG) to support the interim Oversight Authority.

As with other interjurisdictional bodies or those with shared functions between the Commonwealth, states and territories, oversight is determined by both the Commonwealth as well as state and territory governments. Austroads suggests that the Oversight Authority could either be comprised of three separate individuals, being a Chair who is nominated by the Commonwealth and fulfils the majority of the functions outlined in the TDI Bill, and two Deputy Chairs who are nominated by the states and territories (with each receiving a majority or unanimous endorsement of members of the National Cabinet). Conversely, should the Commonwealth wish a single individual to hold this role, the legislation should mirror the provisions of s118 of the *Gene Technology Act 2000*, where the appointment of the regulator must have the support of the majority of jurisdictions.

[5] See Chapter 6, Part 1, *TDI Bill*
[6] See Chapter 4, Part 2, *TDI Bill*
[7] See section 100, *TDI Bill*

3.3 Redress framework

Austroads notes that the TDI Bill places an obligation on accredited entities and relying parties to inform affected users of a security or fraud event and for accredited entities to provide a point of contact for seeking information and support about the incident.[8] The TDI Rules may prescribe additional obligations related to identifying and resolving security and fraud incidents and providing assistance to affected users.

Related to our comments above on the limited oversight our members may have of fraud and security incidents, we note that the ability of accredited entities and relying parties to provide meaningful support to affected individuals is limited by the architecture of the System – the brokered model. Where the interactions of a relying party and accredited entity are mediated by an Exchange which prevents them from identifying each other, the relevant entities may be wholly reliant on the information provided by the Oversight Authority in connection with the incident and any limits placed on the use of this information. The ultimate impact of this will be dependent on the nature of any additional obligations prescribed by the TDI Rules.

3.4 Use of biometric information

Prohibition on the disclosure of biometric information to enforcement bodies

The TDI Bill prohibits the disclosure of 'biometric information' to 'enforcement bodies' for any purpose and irrespective of any other law, warrant, authorisation, or order that would otherwise permit the disclosure.[9] 'Biometric information' is defined broadly as any measurable biometric characteristic that can be used to identify an individual (for example, a 'selfie' captured during the identity verification process) and includes biometric templates. The definition is not limited to biometric information that is used in the System.[10]

Based on this broad definition and the clear intent in section 76(3) to override all other laws, the blanket prohibition on the use of biometric information under the TDI Bill could reasonably be interpreted as applying to digital transactions and other activities involving biometric information that are conducted outside the System. Austroads has assumed this is a drafting error and requests that the TDI Bill is amended to clarify that the restriction on the use of biometrics by enforcement bodies applies only to biometric information collected, obtained or generated in connection with the System and not more broadly. Austroads members rely on law enforcement to have access to this kind of information (where permitted by law) to provide assistance to victims of stolen or compromised identity credentials, including driver licences. It is this capability that makes identities, physical or digital, fraud resilient.

Use of biometric information in the System

Certain accredited entities are authorised under the TDI Bill to collect, use or disclosure biometric information for the purposes of either verifying the identity of an individual or authenticating the individual to their digital identity.[11] Section 79(1) requires identity service providers to delete biometric information collected for the purpose of verifying an individual's identity once the verification process is complete. This deletion requirement does not apply to credential service providers where biometric information is obtained for the purposes of authenticating the individual to their digital identity and the relevant individual has not withdrawn their consent to the use of that information.

[8] See Chapter 2, Part 3, *TDI Bill*
[9] See section 76(2)(a), *TDI Bill*
[10] We note the broader definition of "digital identity information" is defined as information that is generated, obtained or collected in connection with any digital identity system and not the System only. The use of "digital identity information" for enforcement related activities is subject to separate prohibitions in section 81.
[11] See section 77(1), *TDI Bill*

As previously noted, Austroads' members are the custodians of biometric information collected and used for the purposes of issuing and maintaining driver licences and are committed to preserving the integrity and reliability of these credentials. The Position Paper appears to suggest that "metadata and logs" alone could be used to re-establish an individual's Digital Identity with a new identity service provider in the event the original provider was offboarded from the System. This raises questions about how biometric information retained in the System will be used in practice – other than for the narrow testing and fraud prevention purposes. Further detail is required to provide certainty to our members about how biometric information is shared through the System and the standards which apply to this information, in particular user generated images or 'selfies'. Our members are concerned about the use of lower resolution facial images in the System and the possibility such use will supersede the use of higher-state licence images which creates a risk of fraud and identity theft.

We note also that the Biometric Verification Rules in Chapter 5 of the TDIF Accreditation Rules are subject to review. For the reasons noted above, further clarity on these rules is required including in relation to the image quality requirements for images acquired for verification purposes.[12]

[12] We note that the images acquired for verification purposes must meet the minimum standards for biometric matching required by ISO 29794-5, however this is subject to review.

4. General observations

Austroads appreciates the significant progress that has been made in relation to the development of the TDI Bill and associated rules and the technical capabilities of the System.

As reflected in our comments above, there are, however, aspects of the TDI Bill and the operation of the System that require further clarity including, in particular, the management of security and privacy in the System, the costs of participation, the role and function of the Oversight Authority, ongoing oversight of accredited entities and visibility of what other Commonwealth consumers of identity are aiming for. Without further detail it is challenging for our members make informed decisions about accreditation and participation in the System and the associated investment which may be required.

4.1 Coordinated transport agency engagement

There are various state and territory stakeholders with extensive digital identity, credential and service digitisation experience who can provide support across the policy, regulatory, technical, data custodian and service delivery elements of the System which remain under development. Austroads strongly believes that the Commonwealth would benefit from this expertise and the contributions of these stakeholders including our road agency members and their key contacts in adjacent law enforcement and customer service agencies.

The inter-governmental forums currently available to the states and territories in relation to the development of the System and its supporting legislation are limited. Austroads encourages the DTA to ensure a coordinated and effective avenue for providing feedback to and exchanging information is established and timely and meaningful communications are facilitated.

Austroads also appreciates that there is a need for consistent positions on key issues from its members to be provided to enable the DTA to address collective concerns in a comprehensive manner and to effectively manage the associated administrative burden. Drawing on our previous experience in supporting national identity reform, we propose that Austroads works with the DTA on behalf of Austroads' members (as well as other interested agencies where appropriate) to provide consolidated views and information-sharing as part of an ongoing consultation process (including after the passage of the TDI Bill).

Austroads therefore seeks to be included as a member of the DTA's Digital Identity Cross-jurisdictional Working Group (DICJWG). This will provide Austroads with greater visibility of issues impacting the jurisdictions and will enable Austroads to engage with its members more effectively on these issues in order to facilitate coordinated responses for consideration by the Data and Digital Ministers Meeting. Austroads expects that this would involve a similar role to the one it played on the National Identity Security Coordination Group as an agent of road transport agencies in their dealings with the Commonwealth. This approach was highly successful in supporting the work to establish the DVS and other initiatives of the NISSC.

4.2 Role of DVS and NEVDIS

As noted in section 2.1, Austroads has previously worked with the state and territory and the federal governments to develop and operationalise the DVS. NEVDIS, as an aggregated database of registration and licensing data, is a central component of the DVS architecture and provides a single point of interface with the DVS Hub.

The existing DVS operating model and supporting architecture has proven to be a workable and practical identity verification and attribute management solution since its implementation and has the support of the states and territories who provided key inputs into its design. This existing architecture is capable of being scaled to meet the needs of the System and the DVS Hub upgraded to serve as a reliable national exchange. A key benefit of leveraging existing systems is that the application and implementation of the privacy and security protections which currently apply have been tried and tested and are well understood and accepted. The DTA may also wish to consider how Austroads can use its NEVDIS experience to support the aggregation of other credentials such as birth certificates and how resulting repositories can be similarly integrated with the DVS or FVS or both.

For the full benefits of the System to be realised in the long-term and to enable effective participation by the states and territories, Austroads believes that the System should be established in a way that avoids complexity and unnecessary risk and leverages current architecture and systems, with a proven record.

Austroads strongly welcomes further consultation on key aspects of TDI Bill and associated rules and looks forward to the opportunity to further engage on fundamental aspects of the System with the DTA covering policy and technical matters in relation to security, the charging framework, privacy and use of biometrics, governance and oversight.

Appendix A Austroads' role in national identity reform

Our purpose

The Austroads constitution notes that Austroads is established to contribute to development and delivery of the Australasian transport vision and outcomes by:

- supporting the safe and effective management and use of the road system
- developing and promoting national practices, and
- providing professional advice to member organisations and national and international bodies.

As part of these objectives, Austroads aims to provide strategic direction for the integrated development, management and operation of the Australian and New Zealand road and transport system through:

- the promotion of national uniformity and harmony
- elimination of unnecessary duplication, and
- the identification and application of world best practice.

Austroads has a Memorandum of Understanding with the Transport and Infrastructure Senior Officials Committee to deliver national reform projects where Austroads is identified as a suitable vehicle for delivery.

Our role in national identity reform

The concept of a national driver licence exchange was initiated in 1991 by the June Special Premier's Conference which recommended that Austroads develop a plan for a national registration and licensing system.

Since its establishment in 1998, Austroads has hosted the National Exchange of Vehicle and Driver Information System (NEVDIS) on behalf of the eight states and territory jurisdictions who contribute registration and licensing data. NEVDIS is a single consistent national repository of registration and driver licensing information that is owned and managed by Austroads. NEVDIS has been integrated with the Document Verification Service (DVS) since 2009 to support agencies and other authorised users to electronically verify evidence of identity documents and make identity-based decisions. Austroads has invested heavily in the technology that supports NEVDIS and its interface with the DVS.

All state and territory departments that administer their jurisdiction's driver licensing and vehicle registration schemes are signatories to the NEVDIS Participation Agreement. Further detail on the development and use of NEVDIS is set out in B.

As the entity responsible for managing NEVDIS, Austroads has been central to a range of other initiatives since the early 2000s aimed at developing nationally consistent approaches to identity verification. During this period, Austroads represented the interests of registration and licensing authorities in consultation with the Commonwealth on personal identity matters including:

- as a member of the National Identity Security Coordination Group (NISCG) tasked with the development and implementation of the National Identity Security Strategy to support intergovernmental cooperation to strengthen Australia's personal identification process;
- participating in a Commonwealth-funded pilot project to verify approximately 75,000 driver licences against NEVDIS in order to gain the necessary statistics to inform the future of the DVS;

- supporting the then Australian Transport Commission to develop a national agreement for consideration by the relevant transport ministers to ensure interoperability and open architecture of state and territory licensing systems for DVS purposes;

- providing verification services via the DVS as an "issuer agency" on behalf of the relevant RTAs to government agencies in 2009 (and to authorised private sector users following the expansion of the DVS in 2015); and

- commissioning the *National Privacy Impact Assessment for Road Agency Participation in the National Facial Biometric Matching Capability* (2015) for government consideration following the joint Commonwealth and NSW Government review into the Martin Place Siege.

In 2017, the now ceased Council of Australian Government (COAG) agreed pursuant to the *Intergovernmental Agreement on Identity Matching Services* to establish a national facial biometric capability which could be used to support the Face Verification Service (FVS) and other identity matching services.

On behalf of the Transport and Infrastructure Council, Austroads commissioned the *Privacy Impact Assessment: Road Agency Participation in the National Driver Licence Facial Recognition Solution and Face Matching Services* (2016) for consideration by COAG. However, this report does not appear to have been considered by the council and the involvement of the ministerial council and Austroads on digital identity matters has diminished in recent times.

Appendix B NEVDIS development and current use

NEVDIS is the product of that recommendation and a range of associated Austroads' initiatives including the development of the *National Strategy for the Integration of Registration and Licencing Systems* and which led to the commencement of Austroads' *National Driver Licence Checking System* in 1992. The purpose of this system was to prevent the fraudulent use of forged driver licences to obtain legitimate licences.

At around the same time, Austroads worked with the Standing Committee of Transport (a Senior Officials meeting) and the Australian Transport Council (a ministerial council) to commission, and to have each jurisdiction consider, independent cost benefit and feasibility studies for a jurisdictionally integrated registration and licencing system. Following this work, in 1996, the Australian Transport Council approved the development of this system – known today as NEVDIS – for the purposes of, among other things, preventing fraud and allowing for the enforcement of one person, one licence.

NEVDIS consists of two main components:

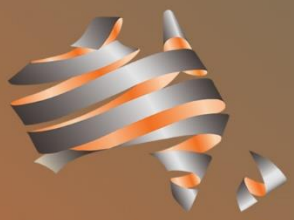
- a Participation Agreement that outlines the conditions placed on members and Austroads to manage NEVDIS Information, and

- an information system that is required to interface with the driver licence and registration systems of the six states and two territories, plus a range of other entities, such as the Australian Criminal Intelligence Commission and the National Heavy Vehicle Regulator.

Today, NEVDIS enables road authorities to interact across state borders and directly supports the transport and automotive industries. NEVDIS has been integrated with the Document Verification Service (DVS) since 2009. The DVS is a secure online system that enables authorised entities to electronically verify evidence of identity documents by confirming that biographical information presented on government issued identity documents (such as diver licences) matches that held by the document issuing agency. This helps the entities to make identity-based decisions by providing greater assurance that the information presented on identity documents is legitimate and linked to the person presenting it. This in turn helps to prevent identity crime, protect privacy and promote greater confidence in the identities that are used by individuals to access government services, and some commercial services.

The DVS verification process requires Austroads, as an "issuer agency" on behalf of the relevant RTAs, to check biographic information provided by a user against licence data held on NEVDIS and to provide a YES / NO response to requesting agencies and authorised private sector users. Austroads discards information provided by requesting parties once the relevant YES / NO response has been processed.

In addition to matching biographic details on driver licenses against data provided by the relevant registration and licensing agencies, NEVDIS collects VIN data for compliance from vehicle wholesalers and stolen information from police and provides information to public and private sector organisations to facilitate provenance checking on vehicles, motor insurance underwriting and vehicle safety recalls.



Austroads

austroads.com.au
Level 9, 570 George Street, Sydney, 2000
+61 2 8265 3300