Thank you for the opportunity to provide a submission to the public consultation on the [*Proposal to make Telecommunications Service Provider (Customer Identity Verification) Determination 2021*](https://www.acma.gov.au/consultations/2021-11/proposal-make-telecommunications-service-provider-customer-identity-verification-determination-2021-consultation-392021#have-your-say).

The Digital Transformation Agency (DTA) supports this proposal to strengthen the fraud prevention measures in place to protect Australians from unauthorised transactions involving telecommunications services and accounts.

The DTA’s submission provides an overview of the Australian Government’s Digital Identity program[[1]](#footnote-2) and how the system could be used to support identity verification of customers under these new rules.[[2]](#footnote-3) Additionally, the submission discusses the Trusted Digital Identity Framework and how it underpins a national approach to digital identity verification.

# **The Australian Government’s Digital Identity program**

Digital Identity provides a simple, accessible and secure way for Australians to verify their identity online.

Creating a standard Digital Identity is similar to a 100-point identification check and provides flexibility for different services that require stronger levels of identity assurance. Digital Identity is entirely voluntary. If a person can’t or doesn’t want to use Digital Identity, they can access services through existing methods such as visiting a shopfront.

Digital Identity does not create a unique identifier, nor does it allow tracking of people’s online activities. It provides a means for people to verify their identity online. An individual ‘owns’ their identity, rather than a unique number ‘owned’ by government. Each time a person uses Digital Identity, they are asked to consent before any details are shared with the service they want to access.

A Digital Identity can be re-used across a range of services, saving people time and effort. Analysis undertaken by KPMG in October 2021 on four digital identity case studies (credit and debit card fraud; KYC obligations; new employee onboarding; SME applications for financial products) estimate economy-wide savings of up to $652 million annually.

Digital Identity is intended to be a whole-of-government and whole-of-economy solution. It is a federated system designed to protect users’ privacy, while allowing access to the broadest range of services possible. The DTA is working collaboratively across Australian states and territories and the private sector to ensure Digital Identity meets user needs at a national level.

More than 6 million Australians are already using their Digital Identity to access over 80 government services. Most of these are business services, for which Digital Identity allows authorised people to assert that they represent a business in a trusted way. Over 1.3 million businesses are currently linked to Digital Identity.

# **How Digital Identity could support the reforms**

The reforms proposed in the amendment will enhance the process in place to verify customers’ identity when purchasing telecommunications services. Digital Identity could play a role in providing telecommunications customers with an option to verify their identity to telecommunications providers in a secure, consistent, convenient, and privacy-enhancing way. Digital Identity can provide strong assurance over a person’s identity at the point of transaction and is supported by embedded safeguards and protections, which will become stronger under proposed legislation.

Any use cases for the Australian Government’s Digital Identity system to be used across the private sector require the passage of Digital Identity legislation (**Trusted Digital Identity Bill**).

# **Reducing fraudulent activity**

Identity theft is fuelling a global increase in cybercrime, fraud, serious and organised crime. Identity verification and digital access are common attack points for fraudulent actors, identity thieves and hackers. Identity crime now impacts one in four Australians, with an annual impact exceeding $2 billion.[[3]](#footnote-4)

Enhanced security provided by Digital Identity could help to minimise the risk of fraud and identity crime in online signature solutions enabling electronic execution of company documents, in the same way it currently supports the more than 80 government services currently connected to the system.

# **Increasing security**

Digital Identity improves the security of transactions for both users and for the services using it by making it much harder for criminals to steal identities. Digital Identity also empowers the user, giving them visibility of their data to ensure it is accurate and will provide them with a history of transactions, including where and when information has been shared, allowing people to check for suspicious activity.

Accredited participants within the Digital Identity system undergo mandatory and regular comprehensive cyber security assessments and penetration tests. These requirements apply to Identity Service Providers, like the government provider myGovID, as well as the exchange and Attribute Service Providers supplying the infrastructure and attributes relied on by connected services. Overseen by the Digital Identity Oversight Authority, the system is continuously improved using the latest cyber security advice, including from the Australian Signals Directorate.

Digital Identity, as part of a solution to verify the identity of telecommunications customers, would extend the strong security processes and procedures already used to protect the most sensitive of government data to these commercial transactions.

# **Improving accessibility**

Digital Identity is both an accessible and secure identification verification process. By no longer needing to present in person, Digital Identity helps to remove one of the biggest accessibility barriers to participation in services and regulatory activities. This includes barriers to the participation in regulated company activities and the execution of company documents.

The DTA has researched and tested the Digital Identity system with real people including those with a disability, older people, and culturally and linguistically diverse users throughout the process. This focus on accessibility helps to ensure that Digital Identity and its connected services are accessible to users regardless of their digital confidence and access to digital platforms. This includes users living in remote areas, those who use older technology or swap between different devices.

# **How the Trusted Digital Identity Framework could support the reforms**

Underpinning the Digital Identity system is the Trusted Digital Identity Framework (**TDIF**) which provides a common technical standard against which providers of identity services can be accredited. This ensures that providers are safe, secure, and accessible and enables interoperability across the federated system.

Even before the passage of the Trusted Digital Identity Bill to roll out the Digital Identity system beyond government services, the TDIF provides a common “rail gauge” for digital identity as it is proven, established, and provides a nationally consistent approach to digital identity. It expands upon sound identity policy already adopted by federal, state and territory governments, such as the National Identity Proofing Guidelines.

TDIF is adaptable and over four major releases it has matured and been used to establish an exchange-based nationally federated model. A fifth release is due in 2022, which aims to incorporate recognition of additional roles and decentralised approaches to identity.

## Whole-of-economy approaches to identity verification

TDIF has stringent privacy, security, and fraud protections to ensure that Australians’ data is protected. Alongside these protections, the TDIF user experience requirements mean that identity services are simple and easy to use and are accessible and voluntary for Australians. It also supports common standards for digital identity proofing, authentication and credential management. The identity documents supported in the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020* are consistent with those supported under the TDIF.

A common approach to digital identity, in particular digital identity proofing, will be key to enabling a national approach. The DTA draws ACMA’s attention to NSW’s support of the TDIF shown through its adoption of the standard in its reforms to age verification for online alcohol sales introduced by the *Liquor Amendment (Miscellaneous) Regulation (No 2) 2021*.

## Multi-factor identity verification requirements

The proposed legislation uses the terminology of “Multi-factor Identity Verification Requirements”. The use of ‘multi-factor’ language risks confusion with ‘multi-factor authentication’ concepts, which users may employ when logging in to devices and services to verify their identity.

## Consistent definitions of identity proofing standards

Identity proofing assurance standards have consistent definitions used by the Australian Government. The intent of Schedule 1 seems aligned to “Identity Proofing Level 2/2+ (Standard strength)[[4]](#footnote-5)”. Stronger online identity proofing assurances (IP3 – (Strong)) have been available via the Digital Identity system since August 2021.

The use of TDIF-accredited, third-party identity service providers by carriage service providers would also remove (or substantially reduce) the requirement for carriage service providers to sight customers’ identity documents, simplify record-keeping requirements and reduce risks associated with secure retention of copies of customers’ identity documents (as mentioned in Part 5).

References to these standards (TDIF, IP levels) may replace tables listing acceptable ‘Category A/B documents’.

## Technology neutral legislation - referencing existing standards

As a federal initiative, it is important that the new rules for telecommunications providers are technology neutral and use consistent and nationally adopted standards, which the TDIF is well placed to provide.

The DTA encourages ACMA to reference the TDIF in the legislative rules in a similar way to NSW’s age verification reforms to ensure that identity verification is being done in a standard, nationally consistent way across Australia. Cross-references to these standards would allow the technical standards and frameworks to evolve in parallel.

For example, Part 2 – Section 10 – Point 3 of the proposed draft could be expanded to include:

(c) using a TDIF-accredited provider of an online identity verification service

This would reflect existing partnerships between Australian telecommunication providers and identity service providers, some of whom are currently undergoing TDIF accreditation[[5]](#footnote-6). Telecommunication providers may also elect to provide a choice of online identity verification providers, one of which could be a government service.

# **Concluding comments**

The Australian Government’s Digital Identity program and the TDIF is well placed to support implementation of these rules.

Digital Identity can deliver better security and fraud control outcomes; leverage common infrastructure; make it easier for people to verify who they are in an accessible, convenient and secure way; and give telecommunications businesses confidence that people are who they say they are.

Thank you for the opportunity to provide a submission. Should the Committee have further questions, please contact [digitalidentity@dta.gov.au](mailto:digitalidentity@dta.gov.au).

Yours sincerely,

Juleigh Cook  
a/g Head, Digital Identity  
Digital Discovery and Sourcing Division  
Digital Transformation Agency  
17 January 2022

1. [digitalidentity.gov.au](https://www.digitalidentity.gov.au) provides information on the Australian Government’s Digital Identity system. [↑](#footnote-ref-2)
2. Use of Digital Identity is voluntary and opt-in, and therefore could only offer one part of a broader solution to identify a person and their intent to sign a document. [↑](#footnote-ref-3)
3. Franks C & Smith R 2020. Identity crime and misuse in Australia: Results of the 2019 online survey. Statistical Report no. 27. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr04732 [↑](#footnote-ref-4)
4. <https://www.digitalidentity.gov.au/digital-identity-for-you/what-are-identity-proofing-levels> [↑](#footnote-ref-5)
5. <https://www.mastercard.com/news/ap/en/newsroom/press-releases/en/2021/september/mastercard-applies-for-accreditation-under-the-trusted-digital-identity-framework-tdif-in-australia/> [↑](#footnote-ref-6)