Australian Government
Digital Transformation Agency

dta

Digital Identity Legislation

A legislative framework for establishing permanent governance structures and privacy protections for the Digital Identity system

Consultation Paper

Digital Transformation Agency

Version: 1801

Contents

1. Glossary of terms

This glossary draws on existing terminology used in the Trusted Digital Identity Framework (TDIF). The definitions set out below are for the purposes of the Consultation Paper only. The Digital Transformation Agency (DTA) does not intend for the definitions in this glossary to indicate how the terms may be defined in the Legislation.

Accredited Participant. An entity that is accredited in accordance with the TDIF to be a part of the system as an attribute service provider, identity provider, credential service provider or identity exchange (as applicable), is listed by the Oversight Authority on a register, and performs the role for which it has been accredited in connection with the system.

Attribute. An item of information or data associated with an individual. Examples of Attributes include information such as name, address, date of birth, email address and mobile phone number.

Attribute service provider. An entity that has been accredited in accordance with the TDIF as an attribute service provider and that verifies specific Attributes relating to entitlements, qualifications or characteristics of an individual (for example, this Joe Bloggs is authorised to act on behalf of business XYZ in a particular capacity).

Biometric Information. Information about any measurable biological characteristics of a natural person that can be used in the system to identify them or verify their identity, such as face, fingerprints or voice.

Biometric matching. The process of automated identification of an individual in the system using their Biometric Information.

Credential. The technology used to authenticate an individual's identity. A Credential may incorporate a password, cryptographic key or other form of access restriction.

Credential service provider. An entity that has been accredited in accordance with the TDIF as a credential service provider and that generates, binds and distributes Credentials to Users or binds and manages Credentials generated by Users themselves.

Digital Identity. A distinct electronic representation of an individual which enables that individual to be sufficiently distinguished when interacting online, including when accessing online services. When capitalised it refers to the electronic representation of an individual whose identity has been verified using the system and when not capitalised it refers to it generically.

Digital Identity system or system. The system for identity management transactions which is the subject of this Consultation Paper and the Legislation.

Document Verification Service. The national online system which enables authorised entities to electronically verify the biographic information of an individual on an identity document issued by a range of Australian state and territory government agencies.

Face Verification Service. The national online system which enables a facial image associated with an individual to be compared against another image of the same individual held in government records (such as documents) of that individual, to help verify the identity of that individual.

Identity exchange. An entity that has been accredited in accordance with the TDIF as an identity exchange and that conveys, manages and coordinates the flow of Attributes and assertions between Accredited Participants and relying parties.

Identity provider. An entity that has been accredited in accordance with the TDIF as an identity provider and that verifies the identity of an individual. An identity provider maintains and manages the identity information of individuals and offers identity-based services.

Legislation. The proposed legislation for the Digital Identity system including primary and secondary legislation.

Operating Rules. The binding rules and procedural requirements for participation in the system set by the Oversight Authority as contemplated in section 3.2.1 of this Consultation Paper.

Oversight Authority. The entity responsible for the administration and oversight of the system.

Participant. The Oversight Authority and each attribute service provider, credential service provider, identity exchange, identity provider and relying party.

Privacy Act. *The Privacy Act 1988* (Cth).

Relying party. An entity listed by the Oversight Authority on a register as a relying party and that relies on verified Attributes or assertions provided by identity providers and attribute service providers to enable the provision of access to a digital service to a User.

Trusted Digital Identity Framework or TDIF. The documents which set out the requirements for accreditation of entities in connection with the system.

User. An individual who interacts with the system by establishing a Digital Identity for the purpose of obtaining a digital service from a relying party.

2. Background

2.1. The need for legislation

The Digital Identity system is a simple, safe and secure way for Australians to verify their identity online. With millions of individuals and businesses already using Digital Identity to access over 70 government services, the Digital Identity system is transforming the way Australians and Australian businesses engage with the government services they use every day. Digital Identity saves individuals time and money and helps businesses and government improve efficiency and productivity.[1]

Currently, only services provided by Australian Government (Government) agencies can be accessed through the system. However, the Government is committed to rolling out a whole-of-economy Digital Identity system to:

- enable Australians to prove who they are online and reduce the administrative burden for small and medium businesses, so they can get on with doing business
- support an increased number of Australians to transact end-to-end digitally, improve privacy and accessibility, and reduce fraud
- enable innovative digital sectors of the economy to flourish.

To facilitate this expansion, the Government is considering the development of legislation which will, amongst other things, establish permanent governance structures for the system as well as enshrine in law a range of privacy and consumer protections in relation to the system. This will ensure the expansion of the Digital Identity system meets the expectations of all Australians and that Users can have confidence in the integrity of the system as it expands.

2.2. How to have your say

The Digital Transformation Agency (DTA) is responsible for the development of the Legislation and is committed to broad consultation in its development, building on the extensive consultation that has been undertaken in the development of the system itself and the underlying policy.

The DTA intends to pursue a comprehensive consultation process in the preparation of the Legislation. This will include a:

- consultation phase ahead of the drafting of the Legislation, including this Consultation Paper, which outlines key issues in relation to the development of the Legislation and poses specific questions about its design, scope and content
- consultation phase following the drafting of the Legislation, which will culminate in consultation on an Exposure Draft Bill, which will seek feedback on the proposed drafting of the Legislation ahead of its introduction.

1 More information on the benefits of Digital Identity to individuals and businesses can be found in the Digital Identity Legislation Background Paper.

Each consultation phase will include several consultation opportunities and mechanisms to ensure it has engaged effectively with stakeholders and the general public on both broad issues and specific topics.

In line with this consultative approach, we are encouraging anyone with an interest in Digital Identity to get engaged in the consultation process in the period ahead, starting with this Consultation Paper.

The Consultation Paper seeks views on key concepts and principles, which will help guide the development, design, scope and content of the Legislation. The Consultation Paper does not represent official government policy but instead outlines a proposed approach to the Legislation for community consideration and feedback. The Consultation Paper is accompanied by a Background Paper, which provides additional details on the Digital Identity system and should be read prior to this Consultation Paper.

We are seeking broad input on this Consultation Paper to ensure the system meets the expectations of the Australian community. If you wish to provide a submission, please read this Consultation Paper and the accompanying Background Paper and consider the questions outlined under each section.

Submissions can made through the Digital Identity website at www.digitalidentity.gov.au.

Submissions will close at 5pm AEDT on Friday, 18 December 2020.

2.3. How your feedback will help

The purpose of this consultation and collecting your submission is to:

- generate public discussion and knowledge about the relevant issues related to the Legislation
- allow the DTA to understand the views of Australians and Australian businesses with regard to the Legislation
- inform the development of the proposed approach in relation to various aspects of the Legislation
- help the initial development of an exposure draft bill on the Digital Identity Legislation.

Your feedback will help us build a strong system that is fit for purpose and aligned with community expectations to support the rollout and adoption of Digital Identity for Australia.

It is your choice whether you provide your personal details with your submission or submit it anonymously. In the interest of transparency, submissions will be made publicly available on the Digital Identity website following consultation, unless you ask for your submission to be confidential.

Further information on how your submission will be treated and your privacy rights can be found in the privacy notice on the consultation submission site, which can be found at www.digitalidentity.gov.au.

3. Overview of the Legislation

3.1. Purpose of the Legislation

The purpose of the Legislation is to:

- enable the Commonwealth, state and territory governments and the private sector to use the system to access (and rely on) identity and Attribute verification services provided through the system
- formalise the appointment and the scope of powers for an Oversight Authority or authorities for the system to ensure it is run efficiently and is trusted
- provide privacy and consumer protections specific to the system, to support and encourage trust.

To achieve the intended purpose of the Legislation, it is proposed the Legislation will provide for the matters set out below.

3.1.1. Legal authority for the expansion, maintenance and regulation of the system

The Legislation will provide the necessary authority for the Government to expand, maintain and regulate the system. The Legislation will allow the system to be used by non-Commonwealth entities including the private sector and states and territories, to access and rely on identity and Attribute verification services provided through the system.

3.1.2. Strengthened privacy and consumer protections

The Digital Identity system is designed to ensure the privacy of Users is protected and strong safeguards are in place to protect data and personal information.

In addition to the existing privacy protections in the Privacy Act, the TDIF currently includes a range of system specific privacy and consumer protections for Users. These protections include:

- restrictions on the creation and use of a single identifier across the system
- restrictions on data profiling
- restrictions on the collection and use of Biometric Information
- requiring express consent before enabling User authentication to a service.

In September 2018, the second Privacy Impact Assessment of the system highlighted strong support for legislation to ensure Accredited Participants are legally bound to key privacy standards specific to the system. Additional Privacy Impact Assessments will be undertaken as we roll out the system, to ensure we are upholding the privacy requirements.

One of the key purposes of the Legislation is to ensure the privacy and consumer safeguards currently contained in the TDIF are enshrined in law, providing enhanced protections for User data and personal information. This will provide clarity for Users around:

- how their data will be used, and the requirement for consent
- who can access their data and in what circumstances, with strict prohibition on misuse
- liability, penalties and redress for fraud or misuse of data.

By enshrining in law privacy and consumer safeguards, the Legislation will instil greater trust in the system as it is rolled out to more services.

3.1.3. Establishment of permanent governance arrangements

Effective governance of the system is essential for the efficient operation of the system and for instilling public trust and confidence.

Currently, an interim Oversight Authority is responsible for the administration and oversight of the system. The interim Oversight Authority's functions are shared by the DTA and Services Australia.

The Legislation will allocate functions, capabilities and powers to a permanent body, or bodies, to act as the permanent Oversight Authority for the system, ensuring it is properly governed and regulated effectively.

These permanent governance arrangements will be designed to provide confidence for Users that the privacy and consumer safeguards enshrined in the Legislation are strictly enforced.

3.1.4. Amendments to other legislation

The Legislation could include amendments to other primary legislation to address provisions which may prevent, hinder or otherwise inhibit the system operating as intended or a Participant from performing their role in the system. This will be explored further as part of the consultation and legislative development process.

Consultation questions:

1A) Are the matters above (legal authority, privacy protections, governance, amendments) relevant matters which should be included in the Legislation?

1B) Are there additional matters which should be considered?

3.2. Structure of the legislative framework

The Legislation will underpin the legal framework for the system. The framework includes:

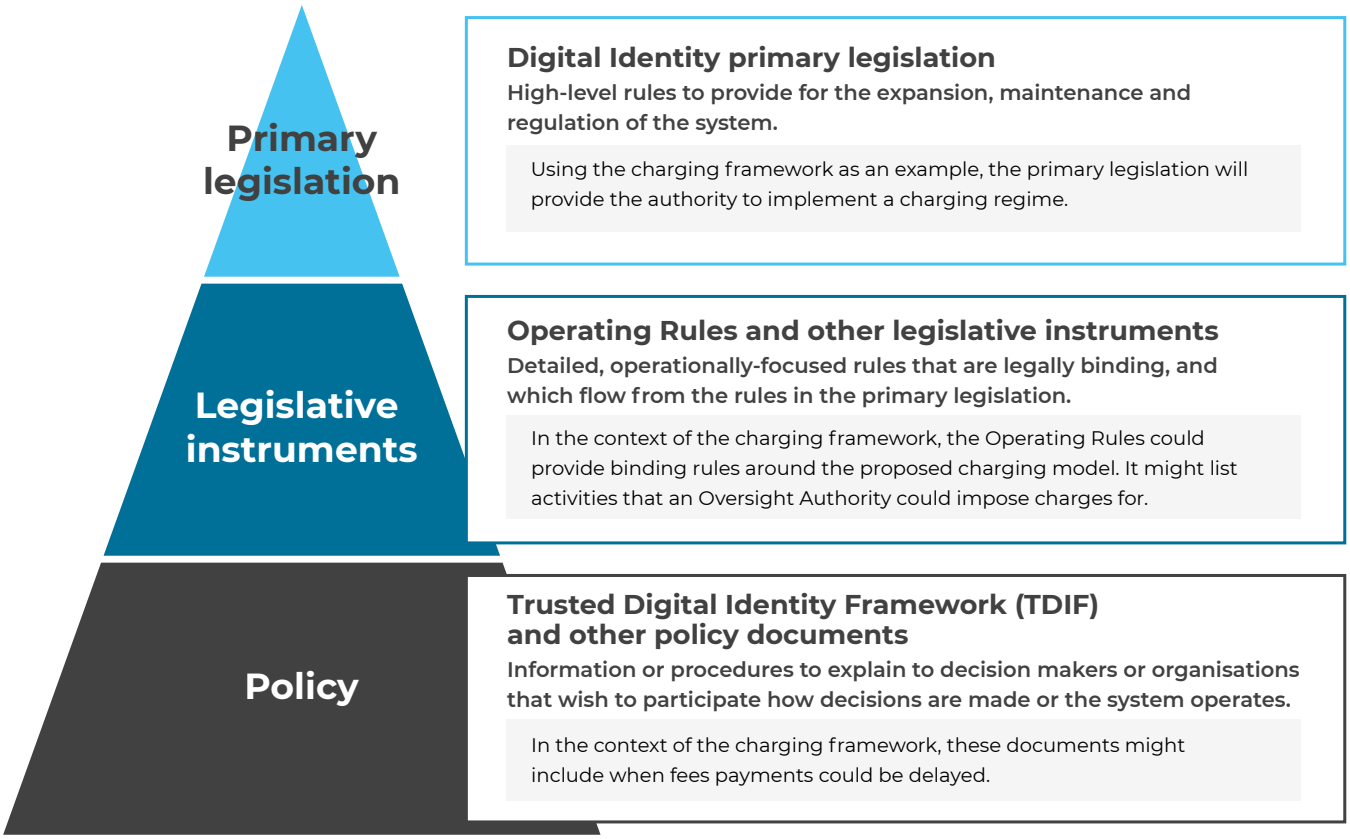
- primary legislation
- Operating Rules and other legislative instruments
- the TDIF and other written policies.

It is expected the primary legislation will include subject matter that will not need to change or that relates to important rights that should only be altered by parliament. An example could be the core privacy protections for Users.

The Operating Rules, other legislative instruments or the TDIF will contain subject matter that is more procedural in nature or that may need to change more frequently. An example may be a security standard for face verification technology.

Some subject matter will have provisions in the primary legislation, legislative instruments and the TDIF/other written policies. This Consultation Paper is concerned primarily with subject matter for inclusion in the primary legislation and Operating Rules/legislative instruments.

The interaction between these components is outlined below.



3.2.1. Operating Rules

It is proposed that the Legislation will provide the Oversight Authority with the power to set and maintain the Operating Rules for the system. It is proposed that the Operating Rules will be set out in a legislative instrument and therefore have the same legal force as the primary legislation.

The Operating Rules will include the binding rules and procedural requirements for participation in the system, including:

- the requirements for the accreditation of entities (by reference to the TDIF) and approval of relying parties in the system
- the ongoing obligations of Accredited Participants to meet TDIF requirements including security, privacy, fraud control and risk management safeguards
- the obligations on relying parties
- the rules around enforcement by the Oversight Authority for non-compliance such as powers to terminate or suspend Participants from the system, issue infringement notices and seek civil or criminal penalties
- the powers of the Oversight Authority to direct or compel information from Participants to undertake inquiries and investigations into their activities
- the mechanisms to support charging Participants and cost recovery.

The Operating Rules will be structured to give certainty to prospective Participants about the requirements for participation in the system. The Operating Rules will also be flexible to ensure scalability of the system as non-Commonwealth entities choose to participate.

3.2.2. The Trusted Digital Identity Framework

Currently, the TDIF sets out the requirements for accreditation of entities in connection with the system. This spans across security, privacy, accessibility, usability, service operations, fraud prevention measures and technical integration matters.

It is proposed the TDIF will continue to set out the minimum requirements entities must meet to achieve and maintain TDIF accreditation. However, some matters currently covered by the TDIF, for example key privacy and security protections, will be included in the Legislation and Operating Rules.

While parts of the TDIF will be enshrined in law, the TDIF will not be a legislative instrument itself, but will remain a standalone and distinct policy. This will allow the TDIF to continue to form the basis for the accreditation of entities, as required by the Operating Rules, and also be a structure for accreditation of entities that do not onboard to the system.

It is proposed the Legislation will provide power for the Oversight Authority to set and maintain written policies, including those aspects of the TDIF that have not been enshrined in law.

This will balance the desire to enshrine in legislation important protections while also maintaining flexibility for existing and potential Participants.

3.2.3. Other written policies

A range of other policy documents could be developed as required to support the Legislation, Operating Rules and the TDIF. Policy documents could provide practical assistance to Participants and digestible information to members of the public who are considering creating a Digital Identity or accessing a service provided through the system.

Consultation questions:

2A) What matters covered by the TDIF should be incorporated into the primary legislation?

2B) What matters covered by the TDIF should be incorporated into Operating Rules?

2C) What matters covered by the TDIF should remain as policy?

3.3. Scope of the Legislation

3.3.1. Who will be covered by the Legislation?

The Legislation will apply to entities which are (or decide to become) involved in the creation, transmission, management, maintenance, use and re-use of Digital Identities, including Commonwealth, state and territory governments and private sector entities. This includes:

- the Oversight Authority established by the Legislation
- entities that are Accredited Participants and relying parties, and who the Oversight Authority lists on a 'Digital Identity Participant Register' (the Register).

The Legislation will not apply to the Document Verification Service or the Face Verification Service. These services are expected to be regulated by their own legislation.

The Legislation will set out the process for the Oversight Authority to allow entities to join the system. The Legislation will also set out the process for entities to exit the system and for the Oversight Authority to remove them from the Register. Any proposed requirements in the Legislation applying to relying parties would continue to apply from the date the Oversight Authority removed them from the Register until the end of a transitional period.

Consultation question:

3) Is a publicly available 'Digital Identity Participant Register' an appropriate mechanism to communicate who will be covered by the Legislation?

3.3.2. Relying parties

The Legislation is intended to build trust for those using the system (Users verifying their identity and relying parties relying on that verification) but is not intended to regulate the services provided by relying parties once an individual has verified their identity. The Legislation is not intended to regulate the quality, security or accessibility of the services provided by relying parties or how Attributes are used by a relying party. Existing laws, such as the Privacy Act, will continue to apply to the activities of relying parties.

However, the Legislation could require relying parties to follow operational obligations that will enhance the system's safety and effectiveness. It is proposed that relying parties will be required to:

- notify the Oversight Authority of any security or fraud events impacting the system and assist with resolution
- comply with any Operating Rules or commercial arrangements applicable to relying parties using the system
- keep their contact details up to date with the Oversight Authority
- meet the extra requirements relating to some Attributes if they are approved to request them (see section 4.43 'Additional restrictions on access to additional Attributes from documents').

Consultation question:

4) Are the proposed obligations on relying parties described above reasonable? Should there be any additional obligations?

3.3.3. What activities will be covered by the Legislation?

The Legislation will apply across the range of activities involved with the system. At the broadest level, the Legislation will set out what a Digital Identity is, who can have a Digital Identity, what a Digital Identity can be used for and any limitations on the use of a Digital Identity.

A Digital Identity:

- will always correspond to only one person, but a person can have multiple Digital Identities with different identity providers
- will always be capable of electronic transmission or its equivalent
- allows a person to access or interact with services offered by relying parties.

The system relies on, and works to further the objectives of, a range of other government policies and initiatives that aim to strengthen identity security and privacy in Australia, such as the National Identity Security Strategy (see Appendix 2). As those initiatives continue to improve the quality and reliability of identity documents used in Australia, the benefits will flow on to the system.

Consultation question:

5) Are the concepts outlined above appropriate to include in a definition of 'Digital Identity' for the Legislation? Are there any additional concepts that should be included?

3.3.4. What information will be covered by the Legislation?

The Legislation will set out the information involved in, or excluded from, the system.

A Digital Identity relies on information about an individual: their family name, given name, date of birth, email address and mobile phone number. The details, or Attributes, used to create, use and re-use Digital Identity involve personal information (as defined by the Privacy Act). If this process involves facial verification, then sensitive information is also involved.

The Digital Identity system also involves information about when a person last updated their email or mobile phone number.

In order to assist a person to access services from a relying party, other pieces of information from identity documents (for example a licence number) held by identity providers may also be passed through the system where a User consents to do so (refer to section 4.4.3). The system will also facilitate an individual acting on behalf of another individual or a business entity.

Attribute service providers can also provide information, such as an individual's qualifications, to relying parties with the individual's consent. Attribute service providers can also facilitate the flow of information about an individual's authorisation to act on behalf of a business entity.

There is already a strong regulatory framework for managing and protecting personal and sensitive information at the Commonwealth and state and territory levels through privacy legislation and policies. A range of other Commonwealth laws, such as the *Social Security Act 1991* (Cth) and the *Taxation Administration Act 1953* (Cth) protect personal information. The proposed Legislation will leverage the frameworks and processes in existing legislation to protect the information the system uses and produces. It is intended that the legislative framework for the system will also create opportunities to support the operation of existing legislation, for example the identification aspects of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

The Legislation will include restrictions on the purposes for which information can be used. Legislation is necessary to establish penalties for misuse or abuse of information used by the system to maintain the system's integrity.

In some cases it may be necessary to specify protections applying to information, to clarify how a penalty or restriction would apply, for example when a person misuses their access and privileged role within an identity provider to link transactions and cause harm.

Consultation question:

6) Does the Legislation need to include a definition of Digital Identity information, or is it preferable to rely on the definitions of personal, sensitive, or protected information in other Commonwealth Acts?

3.4. Financial sustainability of the system

An appropriate charging framework will help ensure the sustainability of the system and its capacity to respond to changes in technology as well as changes in the Australian economy.

The charging framework will need to accommodate and complement the overarching structure of the system, including its federated nature and the fact that an identity provider may not know which relying party has requested the Digital Identity service.

It is intended that the charging framework will have legislative authority and will adhere to Commonwealth Government policies. The specific content of the charging framework in the Legislation will be determined after consideration of stakeholder comments and relevant legal and policy issues.

It is intended that:

- the charging framework will not retrospectively recover the costs of activities related to the design and build of the initial system
- Users will not be charged for the use of a Digital Identity
- relying parties will be charged for the use of a Digital Identity
- the charging framework will cover the range of activities required for the system.

A single charge will cover all Participants' activities, including the Oversight Authority's activities where appropriate. They may include, for example, the activities an identity provider undertakes to create a Digital Identity.

Given the overarching structure of the system, it is likely that a central organisation, such as the Oversight Authority, will need to set the charging framework and distribute funds to Participants, as appropriate. The charging framework will be developed in consultation with relevant parties.

Consultation question:

7) What factors should be considered in the development of a charging framework for the system?

3.5. Liability

Extending the system to provide for state and territory and private sector participation requires the development of an appropriate framework for holding Participants accountable for loss and damage suffered by other entities, including relying parties and Users of the system.

The liability framework for the system will need to:

- be simple to implement and easy to understand
- quickly and appropriately address the concern of the aggrieved party
- ensure continuous improvement of the system as a whole
- ensure proper conduct in the system
- encourage use of the system by relying parties and Users
- ensure the system is affordable, even if loss is incurred
- be transparent.

Where a Participant is to be held accountable, it is proposed the form that accountability could take would include:

- private notice
- public reporting
- financial consequences
- suspension
- termination.

The features of the system the liability framework will need to address include:

Liability allocation

Multiple Participants are involved in the verification of a natural person's identity and there is no single point of accountability/responsibility. Instead, the provision of the 'service' (that is, the verification of a person's identity through digital means) is made up of multiple Participants performing roles in accordance with the system's rules and requirements.

Recoverability

The federated nature of the system, and its technical architecture, affects the ability for aggrieved Participants and Users to recover loss or damage caused by Participants.

It is possible a Participant or User could suffer loss or damage as a result of their use of the system, notwithstanding every other Participant acting in compliance with the system's rules and requirements. It is proposed that Participants would not be liable for loss or damage in such circumstances. However, it is proposed that the liability framework will address circumstances where loss or damage is suffered by a Participant or User and is directly caused by a Participant's failure to comply with the system's rules and requirements.

The liability framework will also need to be developed in the context of the funding and charging framework. In particular, the liability framework will be informed by decisions on who is to be charged and by whom the funds will be collected, and how they will be held and distributed. For example, if relying parties are being charged on a commercial basis for use of the system, they should be able to recover certain losses suffered as a result of their use. Similarly, if identity providers are paid for providing those services, it is proposed they should be (subject to appropriate limits and exclusions) liable for any loss or damage they cause.

The liability framework must interact with any other regulatory powers exercisable by the Oversight Authority under the Legislation (including civil penalties, infringement notices, enforceable undertakings and injunctions) and the rights of administrative review of decisions.

It is intended that the remedies available to Users under the liability framework would supplement, and not replace, those which may be available to Users under other legislation (such as a declaration under section 52 of the Privacy Act that a complainant is entitled to compensation for loss or damage suffered).

Supporting victims of cybercrime and identity theft

The Government is committed to supporting victims of cyber and identity crime. The Cyber Security Strategy 2020 included additional funding for victim support services to assist victims of identity crime, and bolsters cybersecurity support for small and medium businesses. Victims of cyber and identity crime can call the Australian Cyber Security Centre's hotline or iDCare for help recovering their identity.

The TDIF supplements this support by requiring Accredited Participants to address risks of cybercrime and identity theft by:

- demonstrating strong security and privacy safeguards
- having processes for Users to temporarily suspend their account if they think it is being used fraudulently
- providing Users with cybersecurity support services to help Users whose Digital Identity has been compromised (by providing these services themselves or by using third-party services like iDCare).

A User's chosen identity provider is their first port of call if they suspect their identity has been stolen. It is proposed that the Legislation will enshrine the protections contained in the TDIF that require identity providers to 'make good' any circumstance of identity theft by supporting Users to return to the position they were in prior to the theft occurring.

It may be that several different Participants' systems have been involved in a fraudulent transaction, or a User is uncertain who to contact to resolve a problem. It is also proposed that one of the Oversight Authority's functions will be to assist Users to identify the appropriate organisation to contact and support them through the process of recovering their identity.

Consultation questions:

8A) What factors should be considered in the development of the liability framework?

8B) In what circumstances should Participants be held liable under the liability framework?

8C) What remedies and/or redress should be available to aggrieved Participants and Users for loss or damage suffered as a result of their use of the system?

8D) What other best practice mechanisms and processes should be considered to support Users when things go wrong?

4. Safeguards

Safeguarding the personal data of Users is the single most important design feature of the system. The system already includes important technical and policy safeguards designed to protect the personal information of Users. The Legislation will enhance these safeguards and enshrine a range of privacy and consumer protections in law to ensure every Australian can have confidence in the integrity of the system.

4.1. Security

The system is a safe and secure way of proving an individual's identity online. The system has been subjected to comprehensive end-to-end cyber security assessments and risk treatments to improve security and ensure continuing and ongoing security enhancements.

A fundamental security mechanism in the system is the requirement for attribute service providers, credential service providers, identity exchanges and identity providers to obtain TDIF accreditation. To achieve accreditation, these entities are required to demonstrate that their services meet strict requirements in relation to privacy protection, security, risk management and fraud control. To maintain accreditation, Accredited Participants need to continually demonstrate to the Oversight Authority that they meet their TDIF obligations by undergoing annual assessments.

In addition, the system harnesses biometric matching to further enhance Users' security. If, for example, a User's identity documents are compromised and fall into the hands of a fraudster, the requirement for facial verification will mean that the fraudster will be prevented from creating a Digital Identity with medium to high proofing. This will block them from accessing high risk or high value services in the User's name.

Additionally, identity providers may allow a person to use their face or fingerprint to log in to their phone for authentication, which improves login strength. So, while biometric matching is quick and easy for the User, it also helps stop identity crime at both the authentication and verification stages. This paper discusses use of biometric matching and relevant consumer safeguards in section 4.5.

4.2. Privacy

Privacy is a key feature in the technical design and policy framework which underpin the development of the system.

The decision to include specific privacy requirements in the TDIF reflects the commitment to ensuring the system promotes privacy. These requirements impose privacy protections in addition to those contained in the Australian Privacy Principles contained in the Privacy Act, which are also being reviewed (see Appendix 2).

The privacy provisions in the TDIF are designed to address specific concerns around the system relating to:

- possible commercialisation of data and profiling of Users
- the development of a single national identifier or a national surveillance database
- gradual or incremental changes to the system that might result in an erosion of privacy over time
- the use of Biometric Information without clear protections.

All Accredited Participants must meet the TDIF privacy requirements to maintain accreditation. These include meeting the:

- requirements relating to collection, use and disclosure of personal information in the Australian Privacy Principles
- requirements under the Australian Government Agencies Privacy Code 2017 and the Notifiable Data Breaches scheme
- strict requirements around the use of universal identifiers, the use of Biometric Information and to prohibit direct marketing and profiling.

While the TDIF privacy requirements impose a rigorous privacy regime on Accredited Participants, the 2018 Privacy Impact Assessment of the system and TDIF recommended the important privacy protections in the TDIF be enshrined in legislation.

These privacy and consumer protections could include:

- ensuring the system remains voluntary, not mandatory
- prohibition on the commercialisation of personal information and profiling of individuals
- restrictions on the creation and use of a single identifier for the whole system
- restrictions on the use and retention of Biometric Information to those required for verification on the system
- requiring express consent from an individual or their representative to use the system to authenticate and pass Attributes to a service.

Each of the topics is discussed in more detail below.

Consultation questions:

9A) Should the proposed privacy and consumer protections listed above be enshrined in primary legislation?

9B) Are additional protections required? If so, what?

4.3. Choice

Creating and using a Digital Identity is voluntary and completely by choice. Users will have the option to select from multiple identity providers to verify their identity and access government and private sector services online.

A Digital Identity is designed to complement existing identity verification options, such as in-person processes. People will have the choice to set up and use a Digital Identity. They will be able to manage their Digital Identity, including deactivating it, at any time. It will allow a range of government services to be completed end-to-end online, removing the need for people to present in-person at service centres. This is particularly relevant considering the COVID-19 limitations and lockdown requirements currently in place.

For some Australians there may be practical or personal reasons why traditional verification processes are easier or more accessible. As such, relying parties may need to provide an alternative mechanism, such as in-person or paper-based identification and verification options.

For essential and monopoly services, such a requirement could be an obligation. For example, the Commonwealth Government already has obligations to ensure services can be accessed via non-digital channels.

However, there are many smaller public and private sector services that can provide only one mechanism to verify identity. Requiring these types of relying parties to have an alternative to a Digital Identity for an individual to prove their identity (such as a face-to-face or paper-based verification processes) may be unreasonable, given they will need to set up and maintain multiple systems and channels. Therefore, requiring certain relying parties such as local councils, small government agencies or the private sector to provide an alternative channel will not be practical.

Consultation questions:

10A) Should the Legislation include rules around the extent of choice available to Users to verify their identity?

10B) Should any types, or all types of relying parties be obliged to provide an alternative identity verification mechanism, and what exceptions should be available?

4.4. Restrictions on data profiling

The system has been designed with a range of both technical and policy restrictions to limit data profiling. The Legislation will enhance these restrictions and enshrine them in law.

4.4.1. Technical limits on data profiling

Currently, the TDIF prohibits the system creating an identifier for individuals that is used across the system. For example, an identity exchange must create a different identifier for each relying party or identity provider connection relating to an individual. This requirement also prohibits the system creating a new single government identifier. This feature of the system specifically addresses public concerns that the system would create a single, all-encompassing government profile or unique identifier that is used across all of government.

It is proposed that the Legislation will prohibit the creation of a single identifier for individuals that is used across the system.

4.4.2. Policy limits on data profiling

Data profiling limitations are also contained in the TDIF, which requires Accredited Participants to limit the collection, use and disclosure of information about a User's behaviour on the system for the purposes of:

- verifying the identity of an individual and assisting them to receive a digital service from a relying party
- supporting identity fraud management functions
- improving the performance or usability of the Accredited Participant's identity system
- de-identifying the data to create anonymous aggregate data.

It is proposed that the Legislation will place limits on the use of a User's behavioural information collected on the system, especially to prohibit activities such as direct marketing, the sale of information for direct marketing and generalised compliance activities by government.

The TDIF also places limitations on Attributes being passed through the system. The system is designed to be easy for individuals to use when proving who they are to relying parties. One way this is done is by passing some limited and relevant Attributes through the system, so the relying party does not have to request them from the User again.

The TDIF prescribes the list of Attributes that may be requested by relying parties and this list is exhaustive. This means the scope of information available to relying parties through the system is limited to these approved Attributes. Some Attributes will come from identity providers, and others may come from attribute service providers.

Like identity providers, attribute service providers must be accredited against the TDIF before being connected to the system. This will ensure a high level of security and confirm they are a trusted provider of the Attributes they are proposing to provide.

To increase transparency around how and what Attributes are being used by Participants, it is proposed that the Legislation will provide that the Oversight Authority maintain a list in the 'Digital Identity Participant Register' of which Attributes each Participant is approved to receive, with a User's consent, noting the relevant:

- relying party
- data fields
- dates when the Oversight Authority agreed to the relying party having access to the data.

4.4.3. Additional restrictions on access to additional Attributes from documents

Generally, relying parties only receive core Attributes through the system, such as name, date of birth and contact details. However, identity providers will verify other Attributes on documents, such as document numbers. In the TDIF, these are classed as Restricted Attributes.

In limited circumstances, relying parties may apply for access to Restricted Attributes. The Oversight Authority will only grant access where the User has consented to the release, and strict criteria are satisfied, including that the request:

- is in writing
- justifies the reason for requesting the Attributes
- demonstrates the relying party's protective security, privacy and fraud control arrangements are effective and working as intended
- demonstrates why a similar result cannot be achieved without the proposed sharing of Restricted Attributes
- includes a risk assessment
- describes data flows showing how the Restricted Attributes will be used
- demonstrates how the Restricted Attributes will meet a specific legislative or regulatory requirement applicable to the relying party.

For example, a state government service may already request a licence number from a User to verify their identity on their system and this may be authorised under a state law. In that case, if a User has already verified a licence number with an identity provider, that state service could apply for that Restricted Attribute.

In general, the system is designed to avoid poor User experience by not asking a User to have an identity Attribute verified twice – by an identity provider and then a relying party.

Consultation questions:

11A) What types of profiling of behavioural information should be prohibited and allowed?

11B) Should a public register of Attributes be maintained?

11C) Should there be additional restrictions on access to Restricted Attributes?

4.5. Biometrics

Biometric matching technology provides a secure, convenient and reliable way to check that a person is who they claim to be.

Currently, facial verification technology allows Users to prove their identity using the system by comparing a photo of their face taken with their phone, to images in their passport. Over time, this could be expanded to allow Users to prove their identity by verifying their image against their driver's licence photo. The system will only allow a temporary photo of the individual to be matched against an existing verified photo of that person (for example, the passport photo). After the system returns a YES/NO result for the match, the temporary photo is deleted.

The system does not allow a photo to be matched against a database of images (that is, photos of multiple people) to identify an unnamed person. See below for a discussion on 'one to one' matching.

Users who choose to verify their photo documents may use their Digital Identity to access services that traditionally would require an in-person verification of identity, for example by presenting at a government shopfront with photo identification. This will save Users significant time and effort.

It will also greatly benefit people who find it hard to apply for government payments that require identity checks at government shopfronts. This includes people with limited mobility, or who live in remote areas.

4.5.1. Safeguards on Biometric Information

Biometric Information is personally identifiable and cannot be changed easily like an identity document. This means that while Biometric Information can be an important security feature of a digital system, it is essential that it be safeguarded appropriately. It is proposed that the Legislation will limit the use of Biometric Information in the system.

The Privacy Act provides protections for personal information, including additional specific protections relating to sensitive information such as Biometric Information. To complement this, the system places several strong limits on the use of Biometric Information. These include:

- tightly limiting the use of Biometric Information by Accredited Participants to permitted purposes – for example, proofing
- requiring that Biometric Information be deleted by Accredited Participants after it has been used for the purpose for which it was provided, subject to the exceptions discussed in section 4.5.2
- 'liveness' detection to prevent the system being fooled by realistic masks and photos of faces
- strong security and encryption required as a standard
- consent required from the User each time a biometric matching process is conducted by the system
- an easy way for Users to revoke their consent for Biometric Information to be used.

Currently, Users can only choose to use Biometric Information when they are creating a Digital Identity with a high proofing level, or when upgrading their proofing level. For their convenience, they can also use their device's biometrics (for example, FaceID) as part of their authentication credentials. Device biometrics data is not shared with government or any third parties.

In the future, credential service providers may wish to offer Users the choice to use Biometric Information to authenticate to relying parties. Users could instruct their chosen credential service provider to encrypt and securely store their Biometric Information for authentication purposes. This would allow, for example, a User to use their Digital Identity by comparing their voice against the voiceprint held by their credential service provider. Users may be familiar and comfortable with similar processes like using their face or fingerprint to log into their phone.

It is proposed that the Legislation should:

- establish a clear oversight regime for Biometric Information used by the system
- limit the collection of Biometric Information through the system to those Accredited Participants who do proofing or authentication using Biometric Information
- require identity providers or credential service providers to delete Biometric Information once it has been used for the purpose for which it was provided (that is, after an identity proofing process has occurred, or when the User no longer wishes to authenticate using Biometric Information)
- prevent identity providers or credential service providers from sending Biometric Information received through the system to any third parties not required to perform biometric matching or authentication for the User (including relying parties and identity exchanges)
- require identity providers and credential service providers to ask Users for consent each time their Biometric Information is used, ensuring the User is given information about
    - which Biometric Information will be used
    - the duration of the consent's validity
- include penalties for misuse of Biometric Information obtained through the system.

Even with the technical and legislative protections in place, it is proposed that Users will still be able to choose not to provide Biometric Information if they still want a Digital Identity but would prefer to verify their identity offline.

Consultation questions:

12A) Are there any other safeguards on Biometric information that should be included in the Legislation?

12B) Are there any that have been proposed above that should be modified or excluded, and if so, why?

4.5.2. Limitations on accessing Biometric Information

In any digital system that uses Biometric Information, there is a balance between preserving individual privacy and using Biometric Information to make the system more secure, useful and transparent. The system is designed to offer Users the safest, most convenient and transparent system possible. For this to happen, it is proposed that the Legislation would allow highly vetted technicians to randomly sample the Biometric Information on the system for testing purposes.

This would allow for better testing of biometric algorithms, so the system configuration can be optimised. It would also mean that anonymous aggregate information could be used to create more accurate transparency reports, so the public can see how accurate the algorithms are. Without allowing some access by these technicians, any accuracy testing will be approximate, since it will rely on lab experiments rather than actual data.

Where a User has consented for their Biometric Information to be used, it will only be kept while the permitted purpose still exists. However, when sampled with such strict controls, it can still greatly assist to make the system as secure and reliable as possible. As such, it is proposed that the random sampling will only be done with limited sample sizes, for a limited time (with samples destroyed after testing) and conducted after an ethics review.

Users may also want Biometric Information that has been stored for another permitted purpose (that is, for authentication) to help investigators if they are a victim of fraud. For example, if fraud has been committed using a Digital Identity, the victim may wish to allow investigators access to the fraudster's photo collected by the biometric check when the fraudster accessed the account.

Therefore, it is proposed that the Legislation should allow:

- for Biometric Information that hasn't been deleted yet to be randomly sampled for testing and refining the matching algorithms, and to inform anonymous aggregate reporting on biometric accuracy
- an individual who has a Digital Identity to consent for investigators to access stored Biometric Information in relation to a specific fraud or security incident.

4.5.3. Limitations on types of biometric matching

Biometric matching can be used for a variety of purposes, but in the case of a Digital Identity it is only used to help prove an individual is a true and live person. This only requires 'one to one' matching against government identification documents held on file.

It is proposed that the Legislation should limit biometric matching on the system to 'one to one' matching only. This means Biometric Information collected through the system could not be used by identity providers or credential service providers to match against databases or digital galleries containing more than one person's biometric template.

This will mean Biometric Information cannot be used by the system for 'one to many' matching use cases, including:

- **identification of criminals –** use of the system to collect evidence of known criminals trying to access other people's identities or to track people suspected of a crime
- **deduplication of identities –** making sure one person does not have multiple identities under a different name
- **detection of potential fraudsters –** involving the comparison of samples against a watchlist of known fraudsters (particularly where a person is using stolen genuine documents).

Consultation questions:

13A) Do you agree with the proposed approach for Biometric Information?

13B) Will the limitations on Biometric Information overly constrain innovation or rule out legitimate future use cases?

4.6. Consent

The system is built around User consent and the Legislation will embed that concept. A User can choose at any time whether they want to use their Digital Identity to access a service, or use an alternative channel to establish their identity and enable access to the service.

Consent is required at multiple occasions when a person uses the system. A person must consent to set up a Digital Identity with an identity provider. The person's consent must also be obtained by the identity exchange before the person's Attributes can be passed through to a relying party. This is done each time the person transacts with a relying party.

Furthermore, Users can withdraw consent for their Digital Identity to be used at any time, and opt out of the system through a process which is easy to understand and access. When a person chooses to opt out of the system, there will be a need to retain the information from the discontinued Digital Identity for certain specified reasons, such as where the information is needed to investigate allegations of fraud.

The TDIF deals specifically with consent. It sets out a range of high-level rules which require that consent be obtained from a User prior to disclosing the User's Attributes to a relying party or any third party. It also provides that a User must be allowed to withdraw their consent, and the Accredited Participant must maintain auditable logs that demonstrate consent was obtained and is current.

It is proposed that the Legislation will require a User to expressly consent before an Accredited Participant authenticates and sends Attributes to a relying party. This would accommodate a User's ability to provide consent to an identity exchange for Attributes not to be displayed if the User returns to the same relying party (for example, a User could tick a box saying 'do not display next time').

It is proposed that the Legislation will include mechanisms to enable a person to opt out of the system and to disable their Digital Identity at any time.

It may be that, in such cases, the person's Digital Identity is rendered inoperative and can only be accessed in certain clearly delineated circumstances, such as where it is needed to investigate fraud or other criminal activities.

Consultation questions:

14A) Should the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?

14B) Should the Legislation specifically provide an opt-out mechanism enabling individuals to opt out of the system after they have created a Digital Identity?

4.7. Age

There are many examples of situations where a young person may need to access services and where a Digital Identity would facilitate access to those services. A young person may need to have a tax file number (TFN) if they have investments or are in employment. Similarly, recent changes to the law have recognised the right of a young person to have control over their own medical information and to make decisions about their health care.

Allowing a young person to create their own Digital Identity would ensure easier access to the services they require. This gives rise to a range of issues, as the law on the rights of children to make decisions and act in their own right is not uniform across Australia. In fact, different standards are applied in different contexts and across different jurisdictions, with minors able to apply for their own Medicare card or TFN or make decisions about health care at different ages.

Examples of current positions include:

Privacy Act	There is no specific age set to make privacy decisions. This is generally assessed on a case-by-case basis, but in guidance it is presumed a person aged 15 years or over has the capacity to consent, unless there is information that suggests otherwise.
myGov	No age limit applies to myGov, which means that a person can create a myGov account at any age.
My Health Record	Once a person reaches the age of 14, parents will automatically be removed as authorised representatives from the individual's My Health Record and will not have access to the individual's records.
Medical treatment	A young person will be able to consent to treatment if they are considered a 'mature minor' (that is, they have a sufficient understanding and intelligence to enable them to understand fully what is proposed). This depends on a range of factors including the person's age, understanding and the treatment in question.
Tax file number	Anyone can have a TFN. If a person is 12 years old or younger, their parent or guardian must sign the application on behalf of the person. If a person is 13–15 years old, their parent or the person may sign the application. If a person is 16 years old or older, they must sign the application themselves.

The Legislation could deal with the issue of age in several ways, including:

- being silent on the age of a person applying for a Digital Identity in their own right
- setting a minimum age limit for access to the system by individual Users
- setting a minimum age limit for access to the system by individual Users, with override mechanisms to enable the system to be flexible and responsive to the circumstances.

Consultation question:

15) Should there be a minimum age set for a person to be permitted to create their own Digital Identity? If so, what should it be?

4.8. Acting on behalf of another

In some cases, an individual may not be able or willing to engage with the system and may need the assistance of another person to act on their behalf. These situations can be classified into four broad categories:

1. Where an individual lacks the mental or physical capacity and relies on another person (a nominee) to make and execute decisions on their behalf.
2. Where an individual lacks the skills or knowledge required to interact with a government body and authorises a nominee to fill their capability gap.
3. Where an individual prefers to delegate tasks to a nominee due to a lack of motivation or interest in completing the task.
4. Where an individual is too young to create their own Digital Identity, as outlined above.

In such cases, a nominee may be appointed by:

- an individual (for example, an elderly parent who has authorised their adult child to act on their behalf)
- the law (for example, someone with a Power of Attorney, an executor of a will or an Enduring Guardian)
- relationship, either professional or familial (for example, a family member or social worker acting on behalf of a person).

Consultation question:

16) How should the Legislation cover situations where a person lacks capacity, is not capable, is too young or lacks interest or motivation to engage personally with the system?

4.9. Privacy Impact Assessments

Currently, as part of TDIF accreditation, entities seeking accreditation must submit a Privacy Impact Assessment (PIA) for their product. Defined in the Privacy Act, a PIA is a written assessment of a project which identifies the project's impact on the privacy of individuals and sets out a course of action for managing, minimising or eliminating that impact.

Australian Government agencies must conduct PIAs for high privacy risk projects under the Australian Government Agencies Privacy Code. However, this is not an explicit requirement for private sector organisations covered by the Privacy Act, or for other organisations not covered by the Privacy Act. By requiring all Accredited Participants to undertake PIAs, the TDIF expands the protection otherwise offered by the Privacy Act and ensures that all relevant parties have a plan in place to protect individuals' privacy.

Consultation question:

17) Should the requirement for a PIA remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?

4.10. Human rights

The Digital Identity system is an important mechanism by which the Australian Government is working to facilitate fast and secure access to a range of important public services. As such, the use of a Digital Identity will help to facilitate Australians' enjoyment of human rights, including the right to education, the right to health, the right to social services and welfare payments.

In addition, the system engages with the right to privacy, the right to equality and non-discrimination, the right to benefit from scientific progress and the right to equality before the law. The system is also likely to engage with the right to a fair hearing as part of any judicial and merits review of decisions involved in the system.

Given the importance of a Digital Identity for improving access to a range of services, it is important that the Legislation considers how to best support Australians' enjoyment of human rights, and safeguard those rights.

Consultation question:

18) In addition to the right to privacy and anti-discrimination in relation to accessibility and disability, how should the Legislation safeguard and ensure the enjoyment of Australians' human rights?

4.11. Accessibility and anti-discrimination

By facilitating fast and efficient access to a range of services, the system helps to minimise potential discriminatory effects based on age, race, disability, geographic isolation, gender or socio-economic status.

Under the TDIF, identity providers are permitted, and in some cases required, to implement alternative identity proofing processes to assist individuals who face difficulties in providing necessary documents when seeking to verify their identity.

The system is designed and implemented using the Australian Government's Digital Service Standard. The Digital Service Standard requires services to be accessible and inclusive of all Users, regardless of their ability and environment.

The system also conforms with Australian Government requirements to meet the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA. The TDIF also requires identity providers, credential service providers, attribute service providers and identity exchanges to meet User experience requirements, which attempt to minimise any discriminatory impacts on individuals who may not undertake a 'typical' User journey.

It is proposed that the Legislation will include requirements for Accredited Participants to ensure accessible systems and to test the usability of systems with a range of Users.

Consultation question:

19) Is the proposed approach to accessibility and usability practical and appropriate? Should any other considerations be taken into account?

4.12. Penalties

The use of a Digital Identity involves the exchange of sensitive and personal information when a person is seeking to verify their identity online.

Numerous provisions in Commonwealth legislation already prohibit agencies from disclosing sensitive and other personal information, including by imposing sanctions on the disclosure of that information. For example, the Privacy Act promotes and protects the privacy of individuals and would apply to many transactions undertaken under the system. This Act includes a range of enforcement and other regulatory powers, which are based on an escalation model.

However, the Privacy Act currently only applies to 'APP entities', primarily Australian Government agencies and private sector organisations with a turnover of more than $3 million. Certain small businesses are also bound, such as those that provide health services. Generally, individuals are not bound by the Privacy Act.

As discussed in section 6.3 of this Consultation Paper, one option to protect personal information is to prescribe other types of entities as organisations under the Privacy Act, so that those organisations are bound by the Australian Privacy Principles and other Privacy Act protections.

Also relevant is division 372 of the *Criminal Code Act 1995* (Cth), which sets out a range of offences relating to identity fraud. In the context of the system, the most relevant offences include:

- dealing with identification information where there is an intention that a person will commit an indictable offence
- using a carriage service to deal with identification information, where there is an intention that a person will commit an indictable offence
- possessing identification information, where there is an intention that a person will commit an indictable offence.

The Legislation will include additional mechanisms, including penalties for protecting information used in the system, such as Biometric Information. These mechanisms could include criminal offence provisions and civil penalty provisions.

Consultation question:

20) What additional mechanisms, including penalties and redress mechanisms, should be included in the Legislation to prevent disclosure or misuse of personal or other information?

4.13. Disclosure of personal information

The system is designed to protect the personal information of Users involved in creating and maintaining a Digital Identity. The Legislation will expressly prohibit improper disclosure of sensitive or other personal information.

However, there are certain circumstances in which it might be appropriate for information in connection with a Digital Identity to be disclosed. This includes circumstances where a person has consented to the disclosure of their own personal information. In addition to this, there are existing mechanisms in the Privacy Act and other legislation to allow access to information where it is needed to investigate a fraud or criminal offence. It is proposed that these rules would generally apply to the system (except where the Legislation provides otherwise, such as with Biometric Information).

If required, the Legislation could include mechanisms to enable the information protection mechanisms to be overridden in certain circumstances.

Consultation question:

21) Should the Legislation include provisions to enable the disclosure of information in specified circumstances? If so, what should those circumstances be?

5. Governance

Effective governance of the system is essential for its efficient operation and for instilling public trust and confidence.

The system (as a group of Commonwealth entity Participants) is currently governed by an interim Oversight Authority established within the DTA, with operational support functions being delivered by Services Australia. The interim Oversight Authority has a broad range of powers with respect to the safety, reliability and the efficient operation of the system. These include responsibility for:

- accreditation, approval, suspensions and termination of Participants
- monitoring and compliance in accordance with the TDIF and the interim system governance memorandum of understanding between current Commonwealth entity Participants
- management of the Digital Identity Participant Register
- inquiries and investigations of the system including (but not limited to) system incidents, fraud and security
- complaints and issue handling, including complaints from one Participant about another Participant
- preparing and coordinating all public statements and communications in relation to the system.

The Legislation will provide for a permanent, independent Oversight Authority body or bodies with responsibility for the governance of the system. The establishment of permanent, independent oversight of the system will be guided by the following principles, which are discussed in more detail in the sections below:

- Independence
- Transparency
- Accountability

5.1. Independence

To ensure trust in the system, it is important that it is overseen by an independent body or bodies that can investigate any complaints or breaches, among other things. Not only should this oversight be independent, it should also be perceived as independent. Independence in this context is intended to include independence from other government functions and bodies, including other Commonwealth entities.

This does not necessarily require the Government to create a new agency or statutory position – existing agencies or statutory officers could be given appropriate duties and powers to fulfil the necessary functions. The Consumer Data Right legislation provides an example of this approach, where a similar oversight role is shared between the Office of the Australian Information Commissioner and the Australian Competition and Consumer Commission. This may cost less and mean existing mature processes could be used to speed up implementation and provide a ‘one stop shop’ to stakeholders about related issues.

The final structure of the Oversight Authority will be determined by the Government, depending on the functions required and considered through the framework of the Department of Finance's Commonwealth Governance Structures Policy.

Possible governance options for an Oversight Authority could be:

- functions performed by an existing Commonwealth entity or company
- a new Commonwealth entity or company
- a new Corporations Act company (limited by guarantee or shares).

Consultation questions:

22A) Are there established independent bodies that could fulfil the role of an independent Oversight Authority for Digital Identity, or is a new independent body required?

22B) What is the optimal structure of a new body?

5.2. Transparency

The Oversight Authority will be open and transparent about the operation of the system, subject to any confidentiality and privacy requirements set out in the Legislation and Operating Rules. Currently, the TDIF requires identity exchanges to publish in an open and accessible manner an Annual Transparency Report that discloses the scale, scope and reasons for access to personal information by enforcement bodies, as defined in the Privacy Act.

It is proposed that the Oversight Authority would also publish an annual transparency report, and an annual report detailing:

- the names of government agencies and private sector entities using the system
- the number of data breaches (as defined in the Privacy Act) or other security incidents (for example, unauthorised access or disclosure of identity information)
- the number of Privacy Impact Assessments completed
- the accuracy rates of biometric algorithms used by biometric verification services within the system
- the number of successful and unsuccessful proofing requests by Users, with unsuccessful transactions categorised by the reason for non-completion (for example, failed document verification, failed biometric verification).

Consultation question:

23) What type (or types) of information should be required to be publicly reported by the Oversight Authority, to increase transparency in the system?

5.3. Accountability

Guiding Principle Four of the Commonwealth Governance Structures Policy states that governance structures should provide 'appropriate levels of information… to the Parliament and public to enable a clear line of sight between resource decisions and the resulting level of performance'[2].

The Oversight Authority will be accountable to the Parliament and the public, primarily through its accountable authority (for example, its agency head or its portfolio secretary) in accordance with the *Public Governance, Performance and Accountability Act 2013* (Cth), including through periodic and ad-hoc reporting (for example, reporting significant events to responsible ministers and providing public online access to corporate plans and annual reports), attending parliamentary committee hearings and any further requirements prescribed by its enabling legislation.

The Oversight Authority will be subject to periodic review. It is proposed an independent review of the Oversight Authority's performance and the operation of its enabling legislation would be tabled in Parliament three years from the Legislation passing, and then subsequently every five years.

Consultation questions:

24A) What is the appropriate period for review of the governance structure of the Oversight Authority?

24B) Should the Oversight Authority be subject to accountability requirements beyond those in the PGPA Act?

5.4. Functions and activities

In addition to the functions already undertaken by the interim Oversight Authority, the Oversight Authority will have enhanced functions to assist in the oversight and coordination of the relevant entities' use of the system. It is proposed that the Oversight Authority will be responsible for:

- **Accreditation.** The Oversight Authority should administer the accreditation process for Accredited Participants and make an independent assessment of a potential Participant's ability to comply with the requirements of the TDIF before approving its accreditation.
- **Service onboarding.** The Oversight Authority should identify and brief government agencies and private sector entities with the potential to benefit from the system, organise legal documents and assess and approve applications from those wanting to connect to the system prior to commencing technical integration.
- **Fraud and security monitoring.** The Oversight Authority should monitor Participant compliance with fraud, cyber security and privacy requirements. It should also monitor, report, investigate and act on cyber and fraud threats across the system.
- **Service monitoring and incident response.** The Oversight Authority should monitor service availability and coordinate system-wide responses to critical incidents.

2 https://www.finance.gov.au/government/managing-commonwealth-resources/structure-australian-government-public-sector/commonwealth-governance-structures-policy-governance-policy/further-information-key-requirements-governance-policy

- **Customer experience.** The Authority should investigate complaints and coordinate public disclosures and notices related to the system. While Participants should continue to be responsible for complaints and customer support relating to the operation (service quality or availability) of their digital services, complaints and customer support related to the behaviour of Participants (non-compliance) and broader system-related issues should be escalated to the Oversight Authority for investigation.
- **Investigations.** The Oversight Authority should undertake inquiries and investigations into the activities of Participants. It should have powers to access a Participant's records, premises, facilities or systems in connection with their accredited identity service. The Oversight Authority should be able to direct or compel Participants to undertake an action or to provide certain information relevant to system operations or outputs. It is intended that the Oversight Authority would be permitted to use information collected through the system for specific authorised purposes, subject to ongoing regulated use and disclosure of that information by recipients.
- **Enforcing rules.** Where justified, the Oversight Authority should initiate enforcement action against Participants to ensure rules are upheld, and breaches are addressed.
- **Suspension and termination of Participant's use.** The Oversight Authority should have the power to suspend or terminate a Participant's use of the system. This is an essential aspect of ensuring rules are upheld and the system is trusted.
- **Fees and charging.** Subject to further consideration of the charging framework, the Oversight Authority may be best placed to administer charging for identity proofing once the system is sufficiently mature to implement charging arrangements. The Oversight Authority should be able to track transactions between identity providers and relying parties in aggregate for billing purposes.

It is anticipated that the Oversight Authority will rely on the powers available under the Regulatory Powers Act, subject to feedback received through consultation and advice from the Commonwealth Attorney-General's Department.

A comparison of how these functions will build on what the interim Oversight Authority does currently is contained in Appendix 1.

Consultation questions:

25A) Are the roles and functions outlined above appropriate for the Oversight Authority?

25B) Are there any other functions that should be undertaken by an Oversight Authority? If so, what?

5.5. Advisory committees

While the Oversight Authority will retain overall responsibility for the system, it is important that it does so in a collaborative and informed way. One way to ensure key stakeholders are consulted on important decisions is through establishing advisory committees.

Privacy is at the heart of the system. A Privacy Impact Assessment commissioned by the DTA recommended[3] the establishment of a Privacy Advisory Committee made up of eminent privacy professionals and government privacy bodies to advise the Oversight Authority. Accordingly, all potential governance structures should accommodate the Privacy Advisory Committee.

Additionally, it is proposed that a TDIF Advisory Committee would manage the TDIF brand, and the accreditation and management of entities not participating in the system.

Other committees may report to the Oversight Authority to provide expert advice and guidance on aspects of the system, for example a law enforcement or fraud control committee. These committees may or may not need to have roles referenced in the Legislation. The Legislation should allow the Oversight Authority to establish and de-commission committees as required.

Consultation questions:

26A) What other committees or advisory structures do you think may be needed?

26B) Which other organisations or bodies could supply members of the Privacy Advisory Committee?

5.6. Record keeping

Currently the Participants in the system (as a group of Commonwealth entity Participants) have obligations under the *Archives Act 1983* (Cth) to retain records of its activities described in the general records authority (GRA) AFDA Express Version 2.

This GRA includes subjects such as contracts under seal/deeds, external relations, financial management, legal services, strategic management, and technology and information management. If these GRA subjects do not cover the necessary requirements of the system, a specific records authority may need to be developed for the system, which may include provisions to permit the deletion of Biometric Information. It is proposed that the standard period for retention of non-biometric records relating to the system would be seven years.

Consultation question:

27) Should the record keeping requirements be outlined in the Legislation? If so, what should they be?

3 Second Independent Privacy Impact Assessment (PIA) for the Trusted Digital Identity Framework, Galexia (2018), p.14

5.7. Trust mark

The Legislation will create a trust mark to signify that an entity a User is engaging with has passed the stringent accreditation process run by the Oversight Authority. This would allow Australians to recognise legitimate Accredited Participants, and therefore allow them to engage with the system with speed, ease and confidence.

Such a trust mark would need to be protected from misuse, for example by organisations that use it to suggest they are affiliated with the system despite not being accredited by the Oversight Authority. One option for protecting such a trust mark would be to define the mark as a protected symbol in the Legislation. Defining the mark in the Legislation would make it possible to attach criminal penalties to these types of misuse. In turn, this would act as a significant deterrent to misuse of the trust mark, and also make it quicker and easier for the Oversight Authority to intervene and take action against entities that are misusing the mark.

The name of the Oversight Authority may also need legislative protection.

Consultation question:

28) What best practice models should be considered for the protection and use of the trust mark?

6. Interactions with other policies, programs and laws

6.1. Consistency across Australia

As a whole-of-economy solution, the Legislation will interact with other legislation and policies at a Commonwealth, state and territory level.

At the Commonwealth level, it is anticipated that the Legislation may need to include amendments to other existing Commonwealth legislation if that legislation limits the use or disclosure of information which would prevent, hinder or otherwise inhibit a Participant from performing its role in the system.

Commonwealth secrecy provisions are an example of provisions which may have this effect. It is intended that these provisions will be considered on a case-by-case basis and it is not proposed that the Legislation would amend other Commonwealth legislation by way of an all-encompassing override provision.

If a Commonwealth law is generally 'permissive' in relation to decision-making processes for the verification of an individual's identity, it is not intended for the Legislation to amend that legislation to expressly provide for reliance on a Digital Identity. For example, the *Student Identifiers Act 2014* (Cth) provides that an application for a Universal Student Identifier must be made in a manner and form approved by the Student Identifiers Registrar and include any information required by the Registrar. The Student Identifiers Registrar could offer individuals a choice to use their Digital Identity to verify their identity when applying for a Universal Student Identifier. In such cases the Legislation would remain silent.

Inconsistencies between the requirements of the Legislation and other state and territory legislation and policies may arise, as state and territory and private sector entities participate in the system. To balance the desire to encourage participation with the desire for consistency, the following approach is proposed:

1. Where a law or policy is silent or ambiguous and could be interpreted differently by Participants, it is proposed that the Legislation will not generally operate to remove the ambiguity. For example, if legislation sets out a 'permissive' decision-making process, the Legislation will not provide for that decision to be made in a particular way. This is consistent with the proposed approach for permissive Commonwealth laws. However, a preferred position may be articulated in policy to address the ambiguity and provide clarity to Participants about the Oversight Authority's expectation.
2. Where both the Commonwealth and the states and territories purport to legislate or provide a policy position on the same issue but achieve similar outcomes through different processes, it is proposed that the Operating Rules will recognise the equivalent law or policy.
3. Where there is conflict between Commonwealth and state and territory laws, or between programs or policy, it is proposed that the DTA will work with states and territories to assess the extent of any direct conflicts on a case-by-case basis. The DTA will consider the appropriateness of addressing any conflicts in the Legislation based on legal advice.

Consultation question:

29) Is the proposed approach appropriately balanced to achieve the objectives of the system?

6.2. Use of audit logs in judicial proceedings

If someone tries to create a Digital Identity, or to use a Digital Identity to access services, this will create an audit log. Audit logs are likely to be important to establish what did, or did not, happen within the system. As such, audit logs may be useful for investigating or prosecuting fraud.

There is already a well-established body of law in Australia relating to how evidence can and cannot be used in judicial proceedings. Including a position in the Legislation regarding the use of audit logs as evidence in judicial proceedings may clarify the law without requiring initial 'test cases' to establish how they could be treated. Doing so may also benefit Users who suffer a loss in the unlikely event their Digital Identity is taken over or misused.

Consultation question:

30) Should the Legislation specify whether and how audit logs from the system can be used in court as evidence? If so, what should the Legislation say?

6.3. Consistency of privacy protections

6.3.1. States and territories participating in the system

The interaction between state and territory and Commonwealth privacy laws is particularly important to give a uniform level of protection for information used in connection with the system.

Privacy legislation operates in most states and territories. Even for jurisdictions without privacy legislation, there are common guidance documents and non-binding policies which purport to regulate the approach to privacy in specific jurisdictions. However, privacy requirements and enforcement mechanisms vary across jurisdictions to varying degrees. Naturally, it is preferable for privacy provisions to apply as uniformly as possible.

6.3.2. States and territories as Accredited Participants

Users will generally be able to complain to, or seek redress via, the Office of the Australian Information Commissioner (OAIC) about the acts or practices of identity providers, identity exchanges and attribute service providers involved in the system if those acts or practices breach the Privacy Act. However, where Accredited Participants are state agencies this would not ordinarily be the case.

It is intended that for states and territories with privacy legislation, the Legislation will allow state and territory entities to participate in the system as Accredited Participants where their legislation offers equivalent levels of privacy protection to the Privacy Act. An approach to determining equivalence of legislation with the Privacy Act (for example, mandatory data breach reporting requirements), will be considered further in consultation with local and national regulators, and take into account a holistic range of factors.

It is proposed that state and territory entities participating in the system as Accredited Participants in jurisdictions without equivalent privacy legislation will be treated as organisations under the Privacy Act. The Legislation will require specific state and territory entities to be treated as organisations under Section 6F of the Privacy Act to the extent required for activities related to participation in the system. This will result in the entities being bound by the Australian Privacy Principles and other provisions of the Privacy Act where they are engaged in the system.

6.3.3. Private sector Accredited Participants

It is intended that private sector entities offering services as Accredited Participants will be subject to the Privacy Act. In practical terms, most private sector entities offering services as an Accredited Participant are already likely to be large commercial entities with revenue greater than $3 million and therefore will already be subject to the Privacy Act.

However, many companies in the technology sector are small start-ups, and it is possible that a small business may seek to become an Accredited Participant in the system before it reaches the $3 million revenue threshold under the Privacy Act.

It is proposed that the Legislation or Operating Rules would incorporate current TDIF accreditation requirements for small businesses to be subject to equivalent protections in the Privacy Act. Under Section 6EA of the Privacy Act, any small business can choose to be treated as an organisation for the purposes of the Privacy Act. The entity is then covered by the Australian Privacy Principles and other Privacy Act requirements (for example, data breach notification requirements) for all their activities.

Consultation question:

31) Is the proposed approach appropriate to achieve a high degree of consistency of privacy protections?

6.4. Administrative law and judicial proceedings

In the context of the system, the main types of adverse decisions will involve the Oversight Authority denying an application to become a Participant (either an Accredited Participant or a relying party) or relating to revocation of an accreditation or approval.

As a person would be authorised to make particular decisions under the Legislation, those decisions would be subject to judicial review. However, unless the Legislation specifically provides for merits review, decisions made under that enactment would not be subject to merits review.

It is proposed that the Legislation would allow for merits review of Oversight Authority decisions to deny an applicant to become a Participant or to revoke an accreditation or approval.

Consultation question:

32) Should the Legislation specifically provide that additional administrative decisions relating to the system be subject to merits review?

Appendices

Appendix 1 – Comparison of interim Oversight Authority and Oversight Authority arrangements

CURRENT IOA FUNCTIONS TO TRANSITION	FUTURE FUNCTIONS OR ENHANCED CAPABILITIES
Monitor and enforce the system rules (including but not limited to memorandums of understanding and TDIF).	Enhance this capability by allowing the Oversight Authority to issue infringement notices and seek civil or criminal penalties for misuse of the system or non-compliance with system rules.
n/a	Charge Participants for services and recover costs.
Approve a relying party to connect and use the system. Approve the information available for use in the system.	Enhance this capability and regulate it through operating rules.
Suspend or terminate a Participant's use of the system.	Provide avenues for reviews of the Oversight Authority's decision to terminate or suspend.
Investigate cyber security, privacy breaches or fraud incidents.	Enable the Oversight Authority to monitor system activity to detect, investigate, manage and rectify cyber security, privacy breaches or fraud incidents. Enable the Oversight Authority to conduct remote or on-premises audits of Accredited Participants' systems and processes to verify compliance with the Legislation and Operating Rules.
Play a central role in resolving and handling complaints from individuals and Participants in the system.	Enhance this capability by allowing the Oversight Authority to issue infringement notices and seek civil or criminal penalties, to accept and seek enforceable undertakings.

CURRENT IOA FUNCTIONS TO TRANSITION	FUTURE FUNCTIONS OR ENHANCED CAPABILITIES
Approve and Regulate Commonwealth Participants in the system, including maintaining a register of the accredited or approved Participants in the system.	The Oversight Authority establishes and maintains Operating Rules and a Digital Identity Participant Register for all Participants. The Operating Rules build on and extend existing memorandums of understanding. The Operating Rules are likely to be legislative instruments. The Operating Rules will incorporate the Trusted Digital Identity Framework, and its accreditation and ongoing monitoring.
Coordinate responses to security incidents (e.g. data breaches), disaster recovery and other issues that impact Participants in the system.	Enhance coordination capability by providing legislative powers to direct activities of Participants.
Operational activities, User support, provide policy and strategy for the Digital Identity system.	Legislation will allow operational administration of the system to continue.
Manage public communications activities.	Legislation will allow these functions to continue.
Report on the Digital Identity system to the Commonwealth.	Enhance and regulate reporting to the public.
Share data within the Commonwealth to support governance functions.	Share data among all Participants to support governance functions.

Appendix 2 – Other related Commonwealth initiatives

How do the Digital Identity program and the National Identity Security Strategy (NISS) work together?

The Digital Identity program and the National Identity Security Strategy (NISS) are complementary responses to the identity management challenges faced by Australian Government agencies and the private sector.

The Digital Transformation Agency manages the Digital Identity program with support from partner agencies such as the Australian Taxation Office, Services Australia, the Department of Home Affairs, and the Department of Foreign Affairs and Trade.

The Digital Identity program leverages and complements broader inter-jurisdictional work under the NISS. The Council of Australian Governments (COAG) agreed the NISS in 2007 and again in 2012 to improve the integrity of Australia's identity management arrangements. The Department of Home Affairs leads NISS implementation work, in partnership with other Commonwealth agencies and all states and territories.

The National Identity Proofing Guidelines (NIPGs) were developed under the NISS. The NIPGs provide organisations with best practice guidance on how to verify a person's identity. The TDIF adapted the NIPG guidance to apply in the context of the Digital Identity program. Experiences from developing the TDIF will inform future reviews of the NIPGs.

The Digital Identity program uses the Document Verification Service (DVS) and the Face Verification Service (FVS). Home Affairs manages these key initiatives of the NISS in accordance with the Intergovernmental Agreement on Identity Matching Services entered into by COAG in October 2017.

Organisations acting as identity providers in the Digital Identity system use the DVS and FVS to help verify a person's identity. Identity providers match information against one or more of a person's existing government records, before issuing a Digital Identity to a person. Agencies using the DVS and FVS when issuing evidence of identity documents improve the integrity of their records upon which the Digital Identity program relies.

An objective of the NISS is to prevent identity crime and improve the integrity of identity information held by government agencies. The Digital Identity program promotes this objective.

The *Identity-matching Services Bill 2019* (Cth), which is intended to govern the operation of the DVS and FVS, will complement the Legislation, which is intended to govern the operation of the system.

Privacy Act reforms

The Commonwealth Government has commenced a review of the Privacy Act and related laws to evaluate whether Australians' privacy is adequately protected and whether these protections could be improved.

dta

digitalidentity.gov.au