Australian Government

Digital Identity

Your guide to the **Digital Identity legislation**

dta

Digital Transformation Agency

Version: 1801

Contents

1. Minister's foreword

As we have seen during recent years, Australians are keen and willing to adapt to challenges. In recent years, our nation has transformed the way we go about our daily lives – and it all revolves around digital. From shopping to banking to accessing government services, Australia has turned to digital in droves.

With this comes great benefits – a thriving digital economy drives growth by enabling businesses to prosper, providing more job opportunities for Australians, and connecting us with emerging industries and technologies across the world. However, Australians and Australian businesses must have trust and confidence that the system and their personal information is safe and secure.

A safe, thriving digital economy is the best way we can grow the Australian economy.

A safe, thriving digital economy is not possible without digital identity – that is, a safe, secure and convenient way for Australians to prove their identity online.

This is the focus of the proposed Digital Identity legislation. The Trusted Digital Identity Bill, once passed by Parliament, will establish permanent oversight and governance structures for the Australian Government Digital Identity System, and enshrine in law important privacy and consumer protections. It builds on strong safeguards already in place, providing the authority for a consistent set of rules that will protect Australians and Australian businesses. The work achieved in this space, and the future opportunities that legislation will enable, are critical parts of the Morrison Government's ambition for our nation to be a leading digital economy and society by 2030.

The release of this exposure draft of the Bill and supporting materials is the next step in a multi-year journey of consultation to ensure the legislation is robust, fit-for-purpose, and meets public expectations. My sincere thanks to those who have contributed their views to date. I encourage you all to review the materials and provide your feedback to help us ensure this important work is done right.

The Hon. Stuart Robert MP
Minister for Employment, Workforce, Skills, Small and Family Business

2. Statement from the DTA Acting CEO

The Digital Transformation Agency (DTA), in collaboration with other Commonwealth government agencies, is leading the development of the Australian Government Digital Identity System.

Australians are already experiencing the benefits of a world class Digital Identity system, with privacy and consent built in. Over 4 million people and more than 1.2 million businesses using Digital Identity to access 80 government services. This ability to connect people with the government support they need, in a safe, secure and efficient manner, has been critical to the Australian Government's response to the COVID-19 pandemic and recent natural disasters.

The vision for the Australian Government Digital Identity System is a whole-of-economy solution that connects local, state, territory, and private sector services, making a range of activities easier for individuals and businesses. Expanding the System beyond Australian Government services will increase the benefits across the entire digital economy, providing significant economic opportunities and supporting national recovery into the future.

As we increasingly move our lives and businesses online, trust in our digital systems is critical. This is one of the key reasons that the Digital Identity legislation is so important. For the continued safety and security of online digital services, digital infrastructure must be accompanied by legislative safeguards enshrining key governance, privacy, security and integrity principles.

We have undertaken extensive consultation already and have listened to your feedback. We've used your feedback to ensure the draft legislation reflects community expectations and the important principles that will enhance trust in the System.

The release of this exposure draft of the *Trusted Digital Identity Bill* and supporting materials provides another opportunity for you to have your say. We welcome and appreciate your views.

Peter Alexander
Acting Chief Executive Officer, Digital Transformation Agency

3. Using this guide

This guide provides an overview of the materials released for public consultation. It is intended to help you understand and navigate the following documents in the exposure draft package:

Document	Section of this guide
Trusted Digital Identity Bill (or Bill)	7
Trusted Digital Identity Framework (TDIF) accreditation rules	8
Trusted Digital Identity (TDI) rules	9
Regulation Impact Statement (RIS)	10

The guide also provides an update on the development of the charging framework under the proposed legislation (chapter 11).

This guide is not intended to be an exhaustive description of the content of the exposure draft package, as details have been necessarily simplified or omitted. We recommend you read it alongside the source documents themselves, which remain the authoritative description on the proposed laws.

3.1. Where to find more information

To help you understand more about the Australian Government Digital Identity System we recommend reading the following resources that can be found on the Digital Identity website:

- Background paper: for general information about the System
- Position paper: for information on the policies behind the legislation
- Digital Identity website: for information about the existing System

4. Having your say

4.1. Consultation to date

This exposure draft package is the result of more than six years of work and consultation to ensure that the Australian Government Digital Identity System's design, operation, governance and now legislation meets the expectations of Australians and businesses. This includes extensive consultation with the community and industry on the Australian Government's existing Trusted Digital Identity Framework (TDIF) accreditation scheme (which provided the privacy and technology policy basis for the legislation), and a year of specific consultation on the legislation itself.

This exposure draft package release is Phase 3 of our legislation-specific consultation. In Phase 1, we released a consultation paper seeking views on the legislation's possible scope and content. The responses we received were summarised in a synthesis report, and broadly reflected support for System expansion and for certain elements, particularly consumer protections, to be enshrined in law. In Phase 2, we sought feedback on a position paper that outlined key areas of the legislation, including scope, governance, liability and charging. Feedback provided in this second phase has also helped us draft the Bill and supporting materials.

Thank you to everyone who provided feedback throughout the consultation process. There was a range of views expressed and, while not all of them will be reflected in this exposure draft package, we have sought to achieve a reasonable balance between diverse perspectives and the objectives of Digital Identity legislation.

4.2. Providing feedback on the legislation

We want to hear your views on the *Trusted Digital Identity Bill*, the TDIF accreditation rules, the TDI rules and the RIS. These documents are all available on the Digital Identity website.

Our consultation period runs until 5:00 pm AEST Wednesday 27 October 2021. Details on how to provide your feedback is available on the Digital Identity website.

- To provide your feedback on the Bill and associated material simply upload a word document or PDF through our website.
- To help you provide feedback on the RIS, there are four feedback forms available to download from our website. Fill out the relevant form and upload it through our website.

5. The need for legislation

5.1. Providing legislative authority for expansion

Right now, Australians can already use the Australian Government Digital Identity System to access 80 government services. However, legislative authority is required for the Australian Government to expand, maintain and regulate this System. In particular, legislation will allow for the further expansion of the System to state and territory governments and the private sector. This will mean that more Australian businesses, community organisations, state and territory governments and individuals can all benefit from safe and secure identity services.

5.2. Strengthening privacy and consumer protections

To have trust in the Australian Government Digital Identity System, Australians need to know their personal information is securely protected by law.

The Digital Identity legislation enshrines a number of new privacy and consumer safeguards, in addition to the protections which already exist under Australian privacy law. The legislation will require any entity playing a part in the Australian Government Digital Identity System, as well as entities which choose to join the Trusted Digital Identity Framework (TDIF) accreditation scheme, to meet these protections.

The TDIF accreditation scheme offers an opportunity for Australian businesses and organisations to show they can meet high standards of privacy and protective security, even if they are not participating in the Australian Government Digital Identity System. In turn, this provides their customers with confidence that their data is safe.

5.3. Establishing governance arrangements

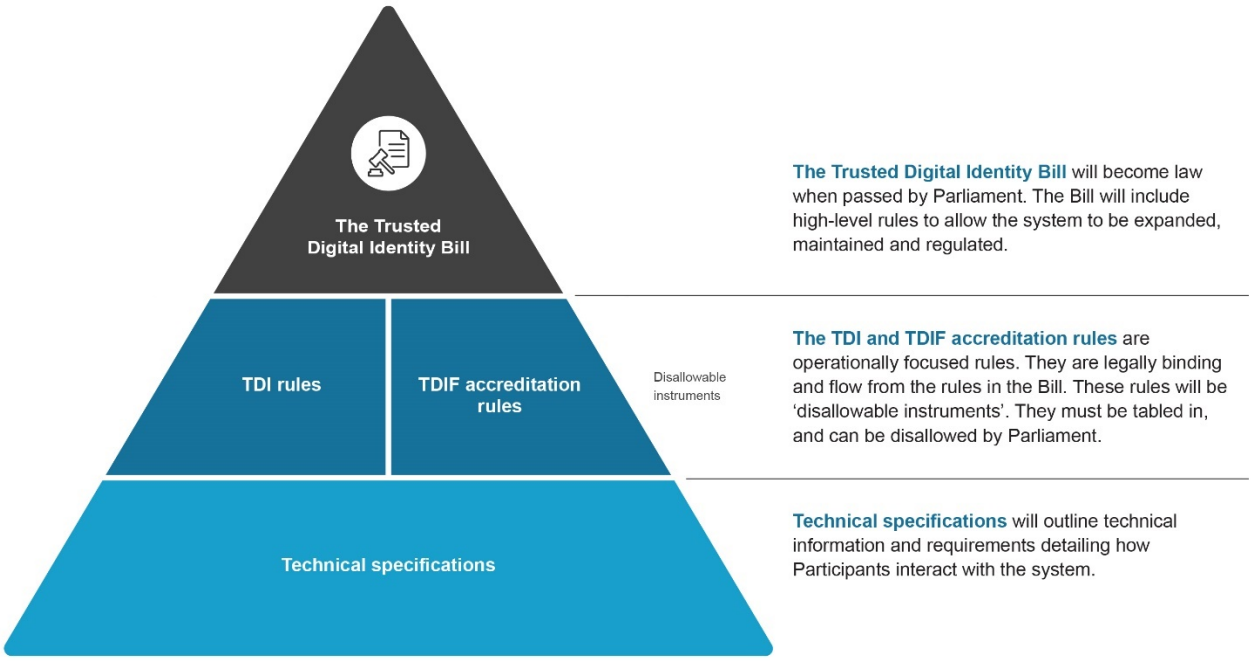
Good governance is essential for the Australian Government Digital Identity System's efficient operation and for public trust and confidence. Legislation will establish a permanent Oversight Authority with responsibility for governing the Australian Government Digital Identity System and the TDIF accreditation scheme under the legislation. The Oversight Authority will be independent, transparent and accountable. The Government is still considering which Government entity will house or support the Oversight Authority.

In addition, the legislation harnesses Australia's existing privacy regulator, the Information Commissioner, to regulate the privacy aspects of the Australian Government Digital Identity System and the TDIF accreditation scheme. This means both schemes will benefit from the experience, staff and expertise of the Office of the Australian Information Commissioner.

6. The legislative framework

The Digital Identity legislation is a package of multiple legislative instruments which, together, form the rule book that governs how the Australian Government Digital Identity System (and other aspects, like the accreditation framework) will work. The different components of the legislation are:

- **Trusted Digital Identity Bill** – proposed primary legislation providing high-level rules for the expansion, maintenance and regulation of the Australian Government Digital Identity System and the TDIF accreditation scheme. The Bill will become law when passed by Parliament.
- **TDIF accreditation rules** – provide the requirements for entities obtaining and maintaining accreditation under the TDIF. These rules are a legally binding instrument which must be tabled in, and can be 'disallowed' by, Parliament.
- **Trusted Digital Identity (TDI) rules** – as above, a legally binding, 'disallowable' instrument, which provide more detail as to the operation of certain provisions of the Bill.
- **Technical standards** (not included in this exposure draft package) – relate to technical integration requirements or technical features for entities to onboard to the Australian Government Digital Identity System. These will be published by the Oversight Authority on its website.



7. Trusted Digital Identity Bill

7.1. Structure of the Bill

The Bill consists of 8 chapters:

Chapter 1: Introduction	**Chapter 5:** TDIF trustmarks
Chapter 2: The trusted *digital identity system*	**Chapter 6:** Oversight Authority
Chapter 3: Accreditation	**Chapter 7**: Administration
Chapter 4: Privacy	**Chapter 8:** Other matters

In this summary, we do not explain concepts in the order they appear in the Bill. Instead, we have bundled concepts thematically to assist your understanding.

7.2. Key definitions

The Bill gives a particular meaning to certain words, which may not be the way that you interpret that word.

From this point in the guide, language used with a specific definition in the Bill is identified in *italic text.*

Below we have extracted and simplified some of the key definitions which are fundamental to the legislation or to helping you understand this guide.

However, it is important to note that we have only extracted a small number of the most important definitions. To properly understand the meaning of any italicised word not defined in this section, you will need to consult the Bill (specifically, Chapter 1, Part 2). You should note that words defined to have a particular in the meaning will have the same meaning in any other related legislative instrument.

In addition, these are simplified descriptions that are designed only to aid understanding. They do not match the exact definitions in the Bill.

- ***Attribute***: an *attribute* of an individual is information that is associated with the individual, and includes information that is derived from another *attribute*. The

legislation provides a non-exhaustive list of *attributes* including first name, last name, date of birth, email address and mobile phone number.

- ***Biometric information*:** a kind of information subject to significant additional protections in the Bill. *Biometric information* is information about any measurable biological characteristic of an individual that could be used to identify the individual or verify the individual's identity (for example, a photo).
- ***Digital identity*:** a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online
- ***Digital identity information*:** includes *attributes*, and is defined as information that is:
  - generated in a *digital identity system* or
  - obtained from a *digital identity system* or
  - collected for the purposes of a *digital identity system*
- ***Digital identity system*:** a system that facilitates or manages either or both of the following:
  - the verification of the identity of individuals
  - the authentication of the digital identity of, or information about, individuals.
- ***Onboarded:*** describes an *entity* which is connected to the *trusted digital identity system*. The definition of *onboarded* prescribes specific circumstances when an *entity* will be considered connected to the *trusted digital identity system.*
- ***Restricted attribute*:** a kind of information which is subject to additional protections in the Bill. The legislation defines *restricted attributes* to include information such as tax file numbers (TFNs), Medicare numbers and health information. Additional *restricted attributes* may be prescribed in the TDI rules after consultation.

See further: Bill Chapter 1, Part 2

7.3. Two voluntary schemes

Key to understanding the Bill is that it enshrines in law two distinct, voluntary schemes which entities can choose to join:

1. **The TDIF accreditation scheme** – an accreditation scheme for providers of identity services, based on the Australian Government's existing Trusted Digital Accreditation Framework (TDIF). Existing accredited entities will be transitioned through to the new scheme.
2. **The *trusted digital identity system*** – the Australian Government run *digital identity system*. This will be the primary source of *digital identity* services for Australian Government entities. Other entities may choose to participate (as providers or consumers of identity services) as well. Entities already providing or receiving services from the existing system will also be transitioned.

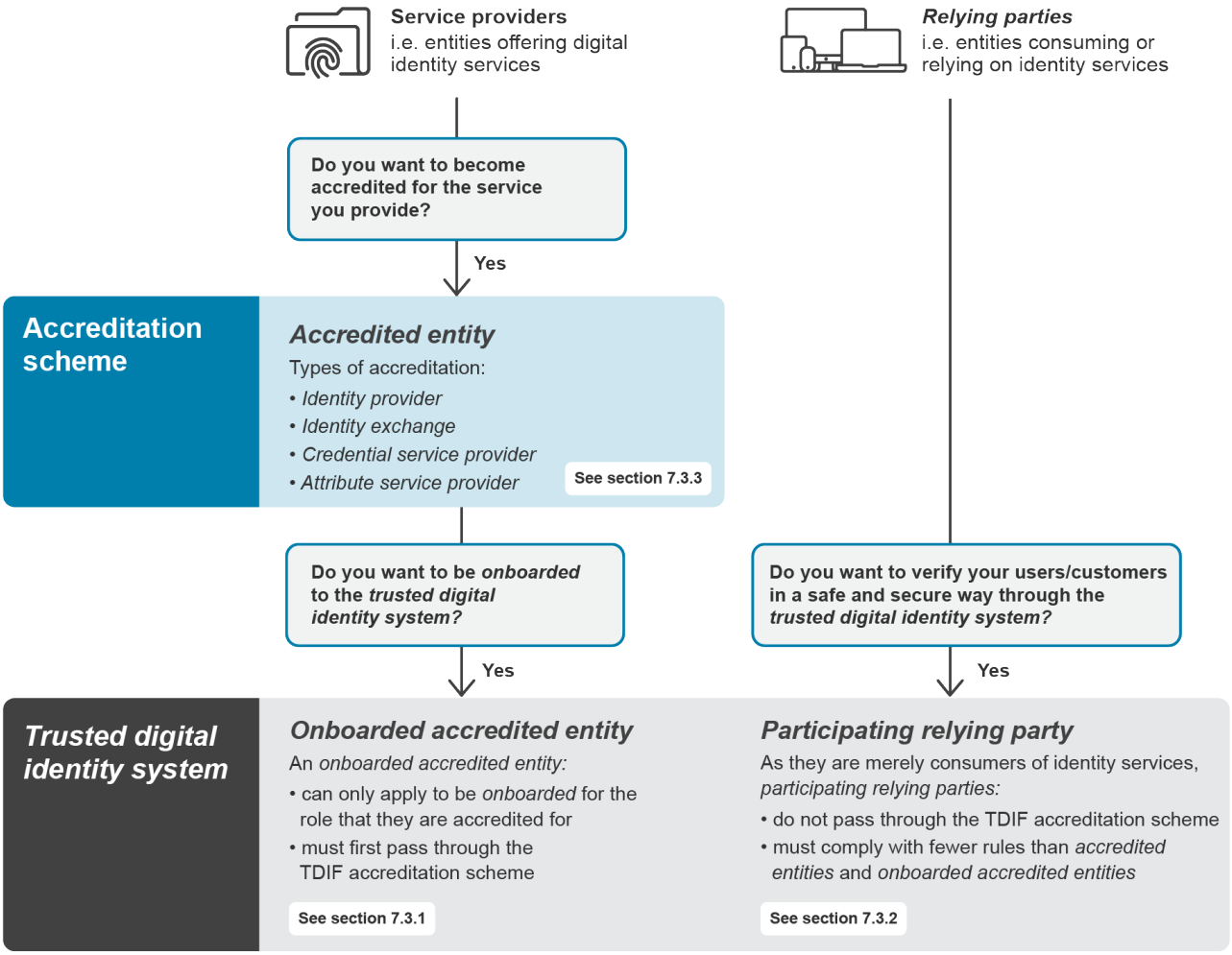
Both schemes entail different benefits and levels of regulation which will affect an *entity's* choice to participate in the *trusted digital identity system*, be accredited or neither.

Notably, the Bill does not prevent *entities* participating in or being accredited under other *digital identity systems* or frameworks while being regulated under either the TDIF accreditation scheme or the *trusted digital identity system*.

In addition, there are two different ways an *entity* can choose to participate in the *trusted digital identity system*:

1. as an ***onboarded accredited entity*** – a service provider offering *digital identity* services in the *trusted digital identity system*. However, to become a service provider in the *trusted digital identity system*, an *entity* must first be TDIF accredited.
2. as a ***participating relying party*** – an *entity* which consumes or relies on the identity services in the *trusted digital identity system* (from the vantage point of an Australian consumer, this is the service that they wish to access online).

The diagram below explains the two different schemes created by the legislation and the different ways of participating.



7.3.1. Onboarding as an *accredited entity*

Eligibility

An *entity* cannot provide identity services in the *trusted digital identity system* (i.e. be *onboarded*) without first being accredited.

Types of onboarding

Under the Bill, an *accredited entity* can only apply to be onboarded for the role that they are accredited for (see accreditation process under section 7.3.3). For example, an *accredited identity service provider* can only apply to be onboarded as an *identity service provider*.

Application process

Applications for onboarding are assessed by the *Oversight Authority*. The Bill outlines a range of matters the *Oversight Authority* may or must consider in deciding whether to onboard an *accredited entity*, including:

- whether the *entity* will be able to comply with the technical standards that apply to it
- whether the Oversight Authority is satisfied that it is appropriate to approve the *entity*
- whether the *entity* is a fit and proper person
- national security considerations.

In addition, an *accredited entity* seeking to onboard may be required to enter into a trusted provider agreement with the Australian Government.

Onboarding conditions

An applicant's approval to onboard is subject to a number of conditions, including that they must:

- meet certain timeframes regarding their onboarding to the *trusted digital identity system*
- comply with service levels
- only onboard as the kind of *entity* for which they are accredited.

The *Oversight Authority* may place additional conditions on an *entity's* accreditation in any category, such as in relation to the kinds of *attributes* that an *entity* can obtain and disclose through the *trusted digital identity system*, or the way in which they can provide their services.

Onboarded accredited entity obligations

The obligations which apply to *accredited entities* continue to apply to an *entity* when it is onboarded to the *trusted digital identity system*. See section 7.3.3 for the obligations that apply to *accredited entities*.

In addition, the Bill requires *onboarded accredited entities* to meet additional requirements and accountability. These include:

- relevant consumer safeguards for the *trusted digital identity system*, including interoperability (see section 7.5.5)
- contacting people using their service if there is a *digital identity fraud incident* or *cyber security incident* affecting them and offer other support to users (see section 7.5.6)
- adhering to the proposed charging framework (see chapter 11)
- adhering to any further rules in the TDI rules (see chapter 9).

See further: Bill Chapter 2

7.3.2. Onboarding as a *participating relying party*

Eligibility

Only Australian entities (including companies, trusts, sole traders, unincorporated associations, partnerships and Australian Government and, state and territory government entities) or foreign companies registered with ASIC can apply to be *onboarded* as *participating relying parties*.

Application process

Applications for onboarding are assessed by the *Oversight Authority*.

The Bill outlines a range of matters the *Oversight Authority* may or must consider in deciding whether to onboard an entity as a *participating relying party*.

Onboarding conditions

Participating relying parties may have appropriate conditions placed on their approval to onboard by the *Oversight Authority*.

Participating relying party obligations

The Bill places a more limited set of obligations on *participating relying parties* than for *accredited entities* or *onboarded accredited entities*. They are:

- comply with relevant consumer protections in the *trusted digital identity system* (see section 7.5.5), including the protection relating to choice on access and voluntariness (i.e. that they must permit the individual to choose which identity service provider they would like to use)
- comply with conditions on their approval
- comply with additional rules in the TDI rules, such as reporting when *digital identity fraud incidents* or *cyber security events* occur (see chapter 9)
- providing certain support to users in the event of a *digital identity fraud incident* or *cyber security incident* (see section 7.5.6)
- complying with service levels set by the *Oversight Authority*.

Suspension or revocation of participation

The Minister can direct the *Oversight Authority* to suspend an *accredited entity's* approval to onboard for national security reasons.

See further: Bill Chapter 2

7.3.3. TDIF Accreditation scheme

Eligibility

Under the Bill, Australian Government, state and territory governments, Australian companies and foreign companies registered with the Australian Securities and Investments Commission (ASIC) can apply for accreditation.

Kinds of accreditation

There will be four kinds of TDIF accreditation when the Bill takes effect. This table offers a simplified description of each kind of accreditation (more formal definitions can be found in section 20 of the Bill):

Kinds of accreditation	What they do
identity service provider	helps a user set up or manage a *digital identity*
identity exchange	facilitates interactions and information-flow between participants in a *digital identity system* (like a switchboard)
attribute service provider	verifies and manages *attributes*
credential service provider	enhances the security and safety of a *digital identity* by managing user credentials (i.e. passwords and other access restrictions)

The four kinds of accreditation under the Bill mirror the four kinds of accreditation under the existing Trusted Digital Identity Framework (TDIF).

Approval process

Applications for accreditation are assessed by the *Oversight Authority*.

An *entity* may only apply for accreditation with the *Oversight Authority*'s approval.

The Bill outlines matters the *Oversight Authority* must consider in deciding to accredit or refuse to accredit an *entity*, including that the *entity* can comply with obligations set out in the Act and the TDIF accreditation rules.

The *Oversight Authority* may also consider whether the *entity* is a fit and proper person, or other relevant matters.

An *entity* may apply to be accredited for just one kind of accreditation, or any number of combination of kinds.

Accreditation conditions

The *Oversight Authority* may place conditions on an *entity*'s accreditation. For example, the Oversight Authority may place a limitation on the levels of identity proofing that an *identity service provider* is allowed to undertake.

Such conditions can be placed on the *entity*'s accreditation at the accreditation stage or afterwards and modified at any time. The *Oversight Authority* will give notice before varying a condition on accreditation.

The conditions will make clear the facility which is accredited and any restrictions on changes to that facility.

Accredited entity obligations

Once they achieve accreditation, an *accredited entity* must adhere to a number of rules in the Bill and legislative framework, including:

- the additional privacy safeguards in the Bill (see section 7.5.1)
- consumer safeguards relating to children, deactivation of digital identities and accessibility of services (see section 7.5.2)
- requirements relating to coverage by the Privacy Act (see section 7.5.3)
- requirements relating to data breach reporting (see section 7.5.4)
- TDIF accreditation rules (see chapter 8)
- requirements relating to the use of trustmarks (see section 7.6.2)

Suspension or revocation of accreditation

Accreditation may be suspended or revoked by the *Oversight Authority* in certain circumstances, including:

- if the *entity* has breached its obligations under the Bill or TDIF accreditation rules
- if the *entity* has been (or will be) involved in a *cyber security incident*
- for insolvency or national security related reasons.

See further: Bill Chapter 3

7.4. Regulation and oversight

7.4.1. Oversight Authority

The Bill creates a new independent statutory office holder called the *Oversight Authority*. The Government is still considering which Government entity will house or support the *Oversight Authority.* There may be future changes to the legislation to support the operation of the functions within the *Oversight Authority*.

The *Oversight Authority* is:

- a person appointed by the Minister for up to five years
- independent and cannot be directed while performing their duties under the legislation
- supported by Australian Public Service staff from an existing Australian Government agency
- supported by an advisory board and any advisory committees appointed by the Minister.

The *Oversight Authority* has many critical roles under the legislation, including to:

- develop, operate and maintain the *trusted digital identity system*
- accredit *entities* for the TDIF accreditation scheme
- approve *accredited entities* and *relying parties* to onboard to the *trusted digital identity system*
- enforce some of the protections in the Bill, such as those related to choice and deactivation of *digital identities*
- assist users in the event of a *digital identity fraud incident* or *cyber security incident*
- maintain the publicly available registers
- help entities covered by the legislation to understand and comply with their obligations
- maintain publicly available registers showing the details of all *accredited entities* and *onboarded* entities
- promote and support *digital identity* matters generally, for example by engaging in promotional and community awareness programs.

To fulfil its functions, the *Oversight Authority* is empowered by the Bill to make certain important decisions and exercise certain discretions, including to:

- make decisions on entities' applications for authorisation to apply for accreditation, accreditation, or onboarding to the *trusted digital identity system*
- revoke or suspend an *entity's* accreditation and/or approval to onboard
- place conditions on an *entity's* accreditation and/or approval to onboard
- allow an *entity* to conduct testing in relation to the *trusted digital identity system*.

The *Oversight Authority*'s powers are discussed at section 7.6.3 in this document.

See further: Bill Chapter 6

7.4.2. Information Commissioner

The Information Commissioner (who leads the Office of the Australian Information Commissioner or OAIC) is Australia's existing national regulator for privacy. It is proposed the Information Commissioner is granted additional functions and powers under the Digital Identity legislation.

The Information Commissioner's key roles under the legislation are:

- to regulate the additional privacy safeguards (see section 7.5.1) and
- to regulate the Privacy Act 1988 in relation to *accredited entities* which are also APP entities (see section 7.5.3).

Other functions or requirements conferred by the legislation to the Information Commissioner are to:

- provide advice to the *Oversight Authority* in relation to matters under the Bill on the *Oversight Authority*'s request
- provide an annual report.

See further: Bill Chapter 4, Part 4

7.4.3. Advisory board

The Minister must establish the trusted digital identity advisory board.

The advisory board has a broad role to advise the *Oversight Authority* on its functions and powers. However, the board may not advise the *Oversight Authority* in relation to certain matters, including on applications for accreditation or onboarding made by entities.

Members of the advisory board:

- are appointed on a part-time basis for up to three years
- must have appropriate qualifications, knowledge or experience
- are governed by additional rules such as in relation to remuneration, leave and conflicts of interest.

See further: Bill Chapter 6, Part 2

7.4.4. Advisory committees

The Minister may establish advisory committees.

An advisory committee advises the *Oversight Authority* on particular issues. The Minister determines the committee's terms of reference.

The Minister determines all matters relating to the appointment of members to the committee.

See further: Bill Chapter 6, Part 2

7.5. Protections

The application of protections in this chapter to different kinds of entities are summarised in the following table:

Type of entity	Protections which apply
Accredited entity (not *onboarded* to the *trusted digital identity system*)	7.5.1 – 7.5.4
Onboarded accredited entity	7.5.1 – 7.5.4 Relevant parts of 7.5.5 Relevant parts of 7.5.6
Participating relying party (*onboarded* to the *trusted digital identity system*)	Relevant parts of 7.5.6

7.5.1. Additional privacy safeguards

The Bill creates eight privacy-related protections (additional to the protection already provided by the federal Privacy Act) to be regulated by the Information Commissioner with its existing and additional powers (see section 7.6.3). These protections apply to all *accredited entities*, whether or not they are *onboarded* to the *trusted digital identity system*.

The table below sets out these protections, and groups some of these together. It contains a heavily simplified explanation of the requirements in the Bill. For further detail on the precise scope and operation of the protections, see Chapter 4, Part 2, Division 2.

Protection	What the Bill requires
Requirement for express consent	When verifying or authenticating an individual, an *accredited entity* must not send the user's *attributes* to a *relying party* without the user's express consent (e.g. the user may be required to check a tick box).
Disclosure of *restricted attributes*	When verifying or authenticating an individual, an *accredited entity* must not: • Send *restricted attributes* of an individual to a *relying party* without the user's express consent

Protection	What the Bill requires
	• send *restricted attributes* of an individual to participating relying parties which do not have the required authorisation from the *Oversight Authority*. The TDIF accreditation rules will set up similar limits to prohibit disclosure of *restricted attributes* by *accredited entities* to *relying parties*.
Prohibition on single identifiers	*Accredited entities* must not pass a user's identifier they create or receive to more than one other accredited participant or *relying party,* unless they satisfy one of the few prescribed reasons for doing so (for example, detecting, reporting or investigating contraventions of the Act). This prohibition is designed to prevent the system being used to support a single identifier of any kind.
Restrictions on *biometric information*	Due to the sensitivity of *biometric information*, the Bill places a large range of safeguards on the use of *biometric information* by *accredited entities*, including: • prohibiting disclosure to law enforcement • prohibiting disclosure to relying parties • preventing one-to-many matching (i.e. conducting a general data base search to find a match against a particular identity) • requiring express consent before collection, use or disclosure • for *identity service providers*, requiring deletion once verification is complete (subject to exception on testing below) • for *credential service providers*, requiring deletion if an individual withdraws consent (subject to exception on testing below) • limiting collection to *accredited identity service providers* and *accredited credential service providers* only. The Bill allows for retention of *biometric information* in narrow circumstances to enable limited operational testing

Protection	What the Bill requires
	and fraud detection activities. The Bill and TDI rules place controls on such testing, including requirements for: • approval from the *Oversight Authority* • testing plans • only certain kinds of testing to be undertaken • deletion of *biometric information* after 14 days.
Prohibition on data profiling	*Accredited entities* must not disclose information about a user's activities (i.e. the individual's access and use of the *digital identity* services provided by the entity) except in permitted circumstances such as using the information to provide services or comply with their obligations.
Prohibition on certain law enforcement purposes	The Privacy Act generally permits disclosure of *personal information* to an *enforcement body* if is necessary for an 'enforcement related activity'. The Bill narrows the scope of such use or disclosure by not allowing *digital identity information* to be disclosed for an 'enforcement related activity', unless: • the *enforcement body* reasonably believes that a person has committed an offence or has breached a law • the *enforcement body* has started proceedings against a person for such an offence or breach.
Prohibition on certain marketing purposes	*Accredited entities* must not use or disclose a person's *digital identity information* for marketing purposes that are unrelated to the *digital identity* services they provide to the user.
Identity exchanges must not retain *attributes*	An *accredited identity exchange* must not retain a person's *attributes* or *restricted attributes* after the end of an authenticated session.

See further: Bill Chapter 4, Part 2, Division 2

7.5.2. Consumer protections for the TDIF accreditation scheme

The legislation creates three additional safeguards to be regulated by the *Oversight Authority* which apply to all *accredited entities* (however civil penalties for breach of the obligations will only apply if the entity is *onboarded*). The table below sets out these protections; however, please note that these are heavily simplified explanations of the requirements in the Bill. For further detail on the precise scope and operation of the protections, see Chapter 4, Part 2, Division 2.

Protection	What the Bill requires
Digital identity de-activation	An accredited identity service provider must, if requested by an individual, deactivate the individual's *digital identity* as soon as practicable after receiving the request.
Accessible and inclusive services	The TDIF accreditation rules can specify standards that must be met with regard to: • compliance with accessibility standards • useability testing • device or browser access.

7.5.3. Compulsory coverage by the federal Privacy Act

The Bill requires any entity applying for accreditation to be covered by the federal Privacy Act, which includes the 13 Australian Privacy Principles (APPs). In other words, an entity cannot be accredited unless they are already covered by the Privacy Act, or they opt in to the rules in that Act.

Additionally, the Bill broadens the definition of *personal information* from the Privacy Act to include *attributes, restricted attributes* and *biometric information* (to the extent they are not already covered by that definition). The effect of this is to ensure that the requirements from the Privacy Act relating to collecting, using and disclosing personal information extend to these three additional types of information.

As many states and territories have existing privacy legislation which governs how state and territory government agencies handle *personal information*, the legislation contains an exemption for these entities. Therefore, state and territory entities are not required to be covered by the APPs if they are already covered by laws which ensure they are meeting a similar level of privacy protection to the APPs.

Conversely, state and territory entities in jurisdictions without privacy legislation have the option of entering into a contract arrangement which requires them to meet the same level of privacy protection as the APPs.

7.5.4. Notification of data breaches

The legislation also imposes data breach obligations on *accredited entities*. The rules applicable to the entity depend on whether the entity is already subject to other data breach legislation:

Type of entity	Obligations
Entities already covered by the federal Privacy Act (APP entities)	• Comply with existing obligations in the federal Privacy Act (relevantly, the Notifiable Data Breach (NDB) scheme). • Give a copy of any data breach notice given to the Information Commissioner under the NDB scheme to the *Oversight Authority* as well.
Entities already covered by a comparable state/territory data breach regime	• Comply with existing obligations under the comparable state/territory data breach regime. • Give a copy of any data breach notice given to the relevant state/territory privacy to the *Oversight Authority* as well.
Entities not already covered by the Privacy Act or a comparable state/territory data breach regime	• The *accredited entity* is treated as if it were covered by the Notifiable Data Breach (NDB) scheme in the federal Privacy Act. This means that that such entities are required to notify the Information Commissioner if they meet the thresholds for reporting a data breach under that Act. • Give a copy of any data breach notice that they give to the Information Commissioner to the *Oversight Authority* as well.

7.5.5. Additional protections for the *trusted digital identity system*

The legislation creates further protections which apply only to *onboarded accredited entities*. The below table outlines these; however, note that these are heavily simplified explanations of the requirements in the Bill.

Further protections applicable to *onboarded accredited entities* are discussed in the section of this guide relevant to the TDI rules (see chapter 9).

Protection	What the Bill requires
Creating/using a *digital identity* is voluntary	A *participating relying party* must not require an individual to generate or use a *digital identity* as a condition of being able to access their services, unless the *participating relying party* has an exemption from the *Oversight Authority*.
Interoperability	Unless granted an exemption by the *Oversight Authority*, *onboarded accredited entities* and *participating relying parties* must not refuse to provide services to other onboarded entities or *participating relying parties.*
Reporting	*Onboarded* entities have to report digital identity fraud incidents or cyber security incidents to the Oversight Authority. See chapter 9 for more detail.

Another protection that will exist in the *trusted digital identity system* is the requirement for the existing Services Australia *identity exchange* to undertake technical blinding. This protection will be contained as a condition on Services Australia's accreditation from the commencement of the Act.

See further: Bill Chapter 2, Division 4

7.5.6. User assistance and support

The Bill creates two layers of support for users:

1. support from *onboarded* entities
2. support from the *Oversight Authority*.

Support from *onboarded accredited entities*

The Bill requires that *onboarded accredited entities* have adequate systems to support individuals and businesses who are affected by a *digital identity fraud incident* or *cyber security incident*. *Onboarded accredited entities* must:

- set up a point of contact to allow affected individuals to seek help
- make sure the point of contact is publicly available (e.g. on their website)
- have and maintain written policies dealing with *digital identity fraud incident* and *cyber security incidents* (which must include timeframes for managing and resolving these).

Additional obligations apply to all *onboarded* entities (onboarded *accredited entities* and *participating relying parties*) in the event of a digital identity related fraud or security incident, including to:

- contact any individual or business whose *digital identity* was affected
- keep the individual or business informed in relation to the incident, including its management and resolution.

In addition, the Bill allows the Minister to specify (in the TDI rules) additional support services which must be offered to affected individuals and businesses.

Support from the Oversight Authority

In addition, the legislation requires the *Oversight Authority* to offer support to individuals or businesses affected by digital identity fraud or cyber security incidents.

The *Oversight Authority* must support users by:

- informing them about support services available
- providing them with the contact details of the *accredited entities* and participating relying parties involved in the incident
- coordinating the collection and sharing of information about the incident between the relevant parties.

The *Oversight Authority* must also monitor and report on the quality of the support services provided by the *onboarded* entities to affected individuals and businesses.

See further: Bill Chapter 2, Part 3

7.6. Accountability and penalties

7.6.1. Registers

The Bill requires the *Oversight Authority* to maintain two registers which must be publicly available on its website at all times:

1. A register of all *accredited entities* (TDIF accredited entities register)
2. A register of all *onboarded* entities (*trusted digital identity system* register)

The Bill outlines the information that each register must contain, such as:

- kinds of activities the entity is allowed to perform
- any conditions imposed on the entity, including the identity proofing and types of credentials that the entity is authorised to provide
- whether the entity's accreditation or approval to onboard has been suspended or revoked at any time.

The Bill requires *onboarded entities* to have some extra details recorded on the *trusted digital identity system* register relating to their onboarding, such as an exemptions to the interoperability obligation granted by the OA, or if they are a participating relying party, details of any other services they will provide attributes to.

See further: Bill Chapter 7, Part 2

7.6.2. Trustmarks

The legislation allows for two types of *TDIF trustmarks* (sometimes known as logos or trademarks) to be created by the TDIF rules:

- TDIF trustmarks for use by *accredited entities* – to allow a user to know that the entity has passed the TDIF accreditation scheme.

- TDIF trustmarks use by *participating relying parties* – to allow a user to know that their identity verification will be conducted in the *trusted digital identity system*.

To ensure that such trustmarks are not misused, the legislation creates two civil offences:

- unauthorised use of a TDIF trustmark
- creating or using a copycat trustmark (i.e. one which could be likely mistaken for a TDIF trustmark).

See further: Bill Chapter 5

7.6.3. Powers of the Oversight Authority

The Bill grants the *Oversight Authority* a range of specific powers to monitor and enforce compliance with the rules in the legislation. The Bill grants the *Oversight Authority* powers to:

- place conditions on an entity's accreditation and/or approval to onboard
- give directions to entities
- require an entity to produce information or documents
- issue a notice requiring the entity to remedy the breach or to undertake a *compliance assessment*
- suspend or revoke an entity's accreditation and/or approval to onboard to the System
- anything else necessary to fulfill its functions.

For matters other than the additional Privacy safeguards, the legislation grants the *Oversight Authority* powers to:

- issue infringement notices
- seek enforceable undertakings
- seek injunctions and

- seek civil penalties (a financial penalty or a fine) from *onboarded* entities which commit the following:

<table>
<tr><th>Conduct</th><th>Penalty units</th><th>Maximum penalty (as at 30 September 2021)</th><th>Regulated by</th></tr>
<tr><td>Onboarding without approval</td><td rowspan="8">200 units</td><td rowspan="3">200 units
For individuals: $44,400

For corporate or government entities: $222,000</td><td rowspan="9">Oversight Authority</td></tr>
<tr><td>(accredited entities only) Failure to comply with redress obligations</td></tr>
<tr><td>Misuse of trustmarks</td></tr>
<tr><td>Failure to comply with directions</td></tr>
<tr><td>Failure to comply with notices to produce documents</td><td rowspan="5">300 units
For individuals: $66,600

For corporate or government entities: $333,000</td></tr>
<tr><td>Failure to keep records</td></tr>
<tr><td>Failure to destroy or de-identify information</td></tr>
<tr><td>Holding digital identity information outside Australia</td><td>300 units</td></tr>
</table>

The Oversight Authority and its staff commit an offence (punishable by 2 years' imprisonment or a civil penalty of 120 penalty units) if personal information or commercially sensitive information is disclosed outside of the conduct of their duties unless a valid exemption applies (for example, they are required to disclose it under another law or the individual to whom the information relates has expressly consented).

7.6.4. Powers of the Information Commissioner

The Bill empowers the Information Commissioner to use their existing powers under the Privacy Act to fulfil its role as regulator of the additional privacy safeguards.

In relation to the additional privacy safeguards only, the legislation grants the Information Commissioner additional powers to:

- seek enforceable undertakings
- seek injunctions
- seek civil penalties – see table below.

Conduct	Penalty units	Maximum penalty (as at 30 September 2021)	Regulated by
Breaches of the additional privacy safeguards	300 units	For individuals: $66,600 For corporate or government entities: $333,000	Information Commissioner

7.6.5. Liability of participants to each other

The Bill leverages the statutory contract model, used in the Consumer Data Right (CDR) legislation.

Each *accredited entity* is taken to have a separate contract with:

- every other *accredited entity* and
- each *participating relying party*.

Under this statutory contract, each *accredited entity* agrees to comply with obligations under the Act and the technical standards.

A party to the contract alleging a breach by another party may apply to the Federal Court for remedies, including:

- compensation
- an order to comply with the contract
- any other order the court considers appropriate.

However, *onboarded accredited entities* will have no civil or criminal liability to other *onboarded* entities in relation to the service they provide in the *trusted digital identity system* provided they meet two criteria:

- they have complied with all their obligations under the Act and
- they have acted in good faith.

8. TDIF accreditation rules

This section summarises key elements of the draft TDIF accreditation rules. The TDIF accreditation rules set out the standards an entity must meet before it can be accredited by the *Oversight Authority*. Under these rules, each entity that applies for accreditation undergoes a range of tests and compliance checks to ensure that its systems, personnel and processes offer sufficient privacy, security and fraud prevention protections.

8.1. Functional requirements

The TDIF accreditation rules include a series of functional requirements that all entities must meet to be accredited, including requirements on privacy, fraud control, protective security, user experience and technical testing. Entities must also undertake a series of functional assessments.

8.1.1. Fraud control

Entities must take reasonable steps to prevent, detect and deal with *digital identity fraud.* Entities are required to conduct a *digital identity fraud risk* assessment and to document (in a fraud control plan) how they will manage *digital identity fraud* risks.

As part of their *digital identity fraud risk* management, entities must appoint a *digital identity fraud* controller and all personnel must complete fraud prevention and management training (with regular training required for relevant personnel). Entities must also have a digital identity fraud control plan, including strategies, controls, risk tolerance and maturity.

The rules provide further detail on the obligations entities have regarding fraud control, including relating to matters such as:

- preventing, detecting, and investigating *digital identity fraud incidents*
- processes and procedures that must be in place to respond to incidents of *digital identity fraud*
- records to keep about *digital identity fraud* matters.

See further: TDIF accreditation rules Chapter 4, Part 2

8.1.2. Privacy

Entities must appoint a designated *privacy officer* and a privacy champion. An entity must have current privacy policies relevant to their activities, develop and maintain a privacy management plan and ensure all relevant personnel complete privacy awareness training.

Entities must also:

- conduct privacy impact assessments for high-risk projects
- have a data breach response management plan
- have a process for allowing individuals to withdraw their consent
- keep records of consent they obtain from individuals
- provide an annual transparency report summarising requests for information from *enforcement bodies* and the *Oversight Authority*.

See further: TDIF accreditation rules Chapter 4, Part 3

8.1.3. Protective security

Entities must take reasonable steps to prevent, detect and deal with security risks. They must conduct a security risk assessment and document in a system security plan how they will manage security risks.

As part of their security management, entities must appoint a *chief security officer* and all personnel must complete security awareness and management training appropriate to their duties.

The rules detail security controls, processes and procedures that entities are required to implement and maintain relating to matters such as:

- access to ICT systems by personnel
- preventing, detecting, investigating and responding to *cyber security incidents*
- ensuring they have robust ICT systems and use cryptography to protect information in transit and at rest
- disaster recovery and business continuity management

- ensuring the ongoing eligibility and suitability of personnel to access *digital identity information*, including pre-employment screening
- keeping records of access to their ICT systems, how they are used by personnel, and actions that occur with *digital identities*.

See further: TDIF accreditation rules Chapter 4, Part 4

8.1.4. User experience

User experience is a key consideration of the accreditation process. The entity's *accredited facility* (or identity app) must be easily understandable and accessible across all supported devices, and there must be additional digital support for users who are unable to interact with the *accredited facility*.

Entities are required to provide users with information to assist them to navigate the identify verification journey. People must be able to provide feedback to the entity on their experience using the entity's *accredited facility*.

As part of their accreditation, entities must undertake usability testing and an accessibility assessment. They must also prepare a journey map that explains how users will interact with their *accredited facility*. They must ensure information provided to users is available in multiple accessible formats, including accessible online formats (such as HTML), large print format, Easy English, and (where requested by the user) braille.

See further: TDIF accreditation rules Chapter 4, Part 5

8.1.5. Technical testing

Entities are required to undertake several technical tests as part of accreditation and to provide the results to the *Oversight Authority*.

These tests demonstrate that an entity's *accredited facility* meets certain technical requirements in the rules, including:

- detecting *digital identity fraud incidents*
- detecting *cyber security incidents*

- keeping audit logs as required
- preventing the registration and use of *digital identities* associated with a *digital identity fraud incident* or *cyber security incident*
- the functionality of identity proofing by the entity's *accredited facility* (for identity providers) and credential creation and management (for *credential service providers*).

See further: TDIF accreditation rules Chapter 4, Part 6

8.1.6. Functional assessments

The rules require an entity to arrange for functional assessments to demonstrate that their *accredited facility*, and processes and procedures, meet the functional requirements for privacy, penetration testing, security and accessibility. The rules detail what these assessments must cover and how to conduct them.

See further: TDIF accreditation rules Chapter 4, Part 7

8.2. Role requirements

Specific requirements apply to each of the accredited roles. As part of their accreditation, an entity must demonstrate they meet these requirements.

The rules also prescribe the features that an entity may be accredited for under TDIF, depending on its accredited role. For example, the different types of proofing levels and credentials that may be supported. An entity must demonstrate that its *accredited facility* complies with the requirements in the rules for the features supported by its *accredited facility*.

See further: TDIF accreditation rules Chapter 5

8.3. Annual assessments

An entity must conduct several annual assessments to maintain its accreditation. These include privacy, security, and usability assessments. The rules outline arrangements to ensure these are appropriately conducted and informed by all relevant evidence. The entity must provide the *Oversight Authority* with a report detailing its response to each assessment.

An entity must also review its risk assessments, plans and controls (for matters including privacy, fraud and security) at least annually, and provide evidence to the *Oversight Authority* that these reviews have been undertaken and, where relevant, any changes made to address matters arising from the reviews.

See further: TDIF accreditation rules Chapter 6

9. Trusted Digital Identity (TDI) rules

The Bill allows the Minister to make additional rules in relation to certain provisions.

The purpose of such rules is to provide regulated entities with further detail about what their obligations are and how to meet them. Breaches of the rules may trigger compliance actions by the *Oversight Authority*.

This section summarises some key additional elements of the TDI rules.

9.1. Applications by relying parties to onboard

Unlike *accredited entities*, relying parties that are approved to participate in the *trusted digital identity system* do not initially undergo an accreditation process under the TDIF accreditation rules. Therefore, the TDI rules set out certain requirements than a *relying party* must meet before being approved to participate in the *trusted digital identity system*. These requirements relate to matters such as:

- interoperability with other participants
- risk assessments
- security
- redress.

These obligations are similar to the requirements for *accredited entities* in the TDIF accreditation rules; however, they are generally less detailed given the different scope of activities performed by *relying parties* in the *trusted digital identity system*. Once a relying party has met the rules and is onboarded, they are a participating relying party.

See further: TDI rules Chapter 7

9.2. Reporting

The TDI rules prescribe arrangements relating to the notification and management of incidents (*reportable incidents*) that have occurred, or are reasonably suspected of having occurred, in relation to the *trusted digital identity system*.

Generally, entities have an obligation to report the following incidents to the *Oversight Authority*:

- *digital identity fraud incidents*
- *cyber security incidents*
- change of control events
- changes to key service providers.

The TDI rules also provide for actions that the *Oversight Authority* must take when receiving reports of such incidents and events.

See further: TDI rules Chapters 10 to 18

9.3. Record keeping

The TDI rules prescribe record keeping obligations for current and former *onboarded* entities.

Current *onboarded* entities need to keep records of *personal information* and user activity for seven years after the user's *digital identity* on the *trusted digital identity system* is deactivated, or after the relevant transaction has been completed.

Former *onboarded* entities need to keep those records for three years from the date the entity's approval to onboard is revoked.

See further: TDI rules Chapter 19

9.4. Storage and handling of digital identity information outside Australia

The TDI rules restrict the holding, storing, handling or transfer of *digital identity information* outside Australia if the information is or was generated, collected, held or stored by *accredited entities* within the *trusted digital identity system*. The TDI rules require that *digital identity information* must not be stored or accessed from outside Australia, unless:

- it is accessed at the request of a user who is outside Australia, or
- the conduct is undertaken to check the credentials of a person.

The *Oversight Authority* may grant conditional exemptions to these requirements on a case-by-case basis.

See further: TDI rules Chapter 9

9.5. User dashboards for identity exchanges

An important transparency and accountability mechanism for users of the System is the ability for them to monitor their interactions relying parties. The TDI rules will set out requirements for onboarded identity exchanges to provide a 'User dashboard,' and details of the functions the dashboard must provide, such as: the user having visibility over the consents they have provided, the user having the ability to revoke their consent from the dashboard, and visibility over requests the user has made to provide their digital identity and the responses to those requests.

See further: TDI rules Chapter 8 and TDIF accreditation rules Chapter 6, Part 6

10. Regulation Impact Statement (RIS)

This section summarises the RIS, explaining what it is, outlining the preliminary findings, and explaining how you can provide feedback.

10.1. The purpose of a RIS

A RIS is a formal document required for any Australian Government decision that is likely to impact businesses, community organisations or individuals. It considers the regulatory, economic, social and other costs and benefits of a proposed course of action (including alternative options) on stakeholders.

For further information, visit Guidance on Impact Analysis webpage on the Office of Best Practice Regulation website.

The RIS available for download now is a preliminary version, not a final document. We are seeking your feedback on this document. Your responses will inform the final version of the RIS, ensuring it incorporates and reflects the views of those potentially affected by future regulation.

10.2.RIS preliminary findings

The Digital Identity RIS examines the case for regulating the *trusted digital identity system*, compared to alternative options (including non-regulation).

It concludes that establishing a dedicated regulatory scheme through legislation is the best option of those considered because it will provide the most positive net benefit to all stakeholders.

The RIS finds that the key benefits of regulating are that it:

- provides the greatest potential benefits for all stakeholders, as it is the only option which facilitates the *trusted digital identity system's* expansion across the economy
- enables the additional benefits of stronger and legally enshrined consumer, privacy and security safeguards, as well as permanent independent governance arrangements.

While the RIS finds that the legislation option will impose costs (on entities to participate schemes created by the legislation), these are considered minimal relative

to the benefits created by the legislation. In addition, only entities that choose to participate in the *trusted digital identity system* or the TDIF accreditation scheme would need to pay these costs, meaning there is no regulatory burden on entities without their consent.

The RIS finds that the regulatory burden is further reduced by the Bill leveraging existing laws wherever possible, instead of creating additional requirements that may duplicate and complicate existing obligations.

See further: RIS sections 3 to 10

10.3. Providing feedback on the RIS

The assessments and conclusions of the RIS are not final. We are seeking your feedback on these, so we can better understand the impact of the legislation on Australians and Australian businesses.

To this end, the RIS contains various consultation questions related to the list of proposed regulatory measures from the Bill, which you are invited to respond to.

We are primarily interested in the regulatory costs incurred by individuals, businesses and community organisations. We have developed high-level estimates of how much we consider it would cost non-government entities to comply with the measures in the legislation and invite feedback on these estimates. The draft Bill does not impose any regulatory requirements on individuals, so it is not expected that they (whether users or non-users of the schemes in the legislation) will incur any costs.

We have developed a series of feedback forms depending on whether your entity would seek to be a *participating relying party*, accredited *trusted digital identity system* participant or *accredited entity*. A 'General' form is also available if you are unsure of your entity's future potential role. Details on how to provide your feedback is available on the Digital Identity website.

See further: RIS sections 11 and 12

11. Charging framework update

The Bill authorises the Australian Government to make rules related to charging for the *trusted digital identity system*.

It is intended for end users not to be charged to access the *trusted digital identity system*. As such, charging rules will be focused on charging arrangements between providers and services using the *trusted digital identity system.* The overarching purpose of the rules is to ensure the long-term sustainability of Digital Identity in Australia.

We are not releasing charging rules as part of the exposure draft package, however this section is designed to give you an update on the work we have been doing on this topic, including our consultation to date.

11.1. The need for a charging framework

To date, the Australian Government has funded the *trusted digital identity system's* design, development and operation. As it expands, a longer-term approach to funding a whole-of-economy platform is required.

We are in the early stages of developing a charging framework that will provide ongoing, long-term financial sustainability for the *trusted digital identity system*, balancing the need for market maturity with the capacity to meet changing community needs over time, and providing commercial opportunities for private sector participants. A fair and robust charging framework will help ensure the *trusted digital identity system* can support whole-of-economy adoption, while upholding the strict technical and security controls required.

The charging framework will be enabled by the Bill and will be aligned to market-based pricing to encourage *trusted digital identity system* adoption.

11.2. Charging framework development

Development of the charging framework is being shaped by various principles and strategies, as well as ongoing research. In line with the Australian Government Charging Framework and related guidelines, the *trusted digital identity system* will only charge what is required to meet the cost of its operation. A set of cost recovery

principles has therefore been established to support the charging framework development. These principles are reflected in the Bill.

Also underpinning development of the charging framework are four key strategies. These aim to encourage use of the *trusted digital identity system* by early adopters and provide certainty to end users and services alike. They are:

- **Encourage participation:** Creating a framework that promotes and supports greater adoption and use of digital identity.
- **Scalable and adaptable:** Initial charges will be based on reasonable, long-term financially sustainable costs that are fully compliant with the government's competitive neutrality policies.
- **Financially sustainable:** Once a mature state has been reached, charges will ensure the long-term financial sustainability of all participants without requirement for supplementation from government.
- **Simple and transparent:** The initial framework adopts a simple catalogue of services and charges that may be refined over time to better reflect the costs incurred and value received by various stakeholders.

Additional domestic and global research is continually being conducted to inform and support the development of the charging framework. The focus of this research is on understanding possible charging models, as well as market growth and transformation activities which will inform the approach and timing of when a framework could be introduced.

11.3. Next steps

A preliminary view of a charging framework has been developed in consultation with system participants. We will continue to consult with partner agencies, states and territories, and private sector stakeholders to validate and refine this. Outcomes from this consultation will be used to inform the services, charging components and mechanisms required to support a whole of economy charging framework.