Australian Government

Digital Identity

Consultation Regulation Impact Statement

Regulation of the Australian Government Digital Identity System

dta

Digital Transformation Agency

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, please contact the Communications team, Digital Identity and myGov at digitalidentity@dta.gov.au.

Version: 1801

Contents

1 Executive summary

The Digital Transformation Agency (DTA), in collaboration with other government entities, is leading the development of a national federated Digital Identity System (the System). The System uses a decentralised model where people, organisations, services and devices can trust each other because authoritative sources establish and authenticate identities. The System is currently used by over 3.3 million people and over 1.3 million businesses to access more than 77 digital Australian Government services (source: Digital Transformation Agency 2021, *Objective 3 - You will be able to choose a secure and easy-to-use digital identity to access all digital government services*.)

The vision for the System is that people will be able to verify their identity with their choice of identity providers to create a Digital Identity. They will be able to safely reuse that Digital Identity to transact across all tiers of government and with private sector services, in a way that ensures their privacy. Australia's Data and Digital Ministers have agreed to work towards a consistent approach for Digital Identity across Australia. This means the future System will have domestic interoperability across states and territories. Mutual recognition work is under way with other jurisdictions (e.g. New Zealand and Singapore). These efforts build on current experience working with international identity partners, including through the Digital Government Exchange (DGX) and the Organisation for Economic Development (OECD).

Having delivered the foundational capability and infrastructure, governing policy, security and risk management framework, and underlying operational support, the Digital Identity Program (the Program) received two years of funding in the 2020-21 Budget to expand the System. This expansion will focus on making the System available as a 'whole-of-economy solution', enabling all individuals and businesses to have more secure and convenient engagement with government (including state, territory and local) services and the private sector.

Expansion of the System forms a critical part of the Australian Government's Digital Economy Strategy, which aims to secure access to digital technologies and skills for all businesses and individuals, make government service delivery frictionless and integrate data and technologies to make life easier.

The potential for the System has been clearly demonstrated during Australia's response to the COVID-19 pandemic, which has seen an unprecedented increase in the use of digital channels throughout the implementation of JobSeeker, JobKeeper and other stimulus measures. Research has estimated the potential whole-of-economy benefits of extending full System coverage across Australia as between $2–$11 billion, or 3–13% of GDP. (Research on the whole-of-economy value of Digital Identity, and the specific scope and parameters of this analysis, is discussed further at Section 2.5. The case for expanding the System.) Expansion to state, territory and local governments presents efficiency opportunities across the multiple touchpoints between individuals and these entities (for example in licensing regimes, using information from registers of births, deaths and marriages, healthcare, education and utilities). However, even without this expansion, the System is a viable way to deliver Australian Government digital services more efficiently.

To date, the Australian Government has built the foundations of a trusted, nationally consistent identity verification system. However, several risks and gaps have been identified with the potential to impact the full realisation of Digital Identity's benefits, particularly as it expands across the Australian economy. These are:

1. the absence of legal authority for participation of non-Government agencies in the System as relying parties (providing online digital services to people with a digital identity), and for a charging framework
2. a potential lack of trust in the System's privacy and security safeguards
3. the absence of a permanent oversight body and legislative governance framework.

Regulatory action is required to address the gaps identified above, enabling non-Government participation and legislatively entrenching privacy, security and permanent governance arrangements to enhance confidence and trust in the System. Three options have been considered to address the above problem areas – status quo (i.e. no regulatory action taken), leveraging existing regulatory schemes (primarily addressing privacy-related issues) and establishing a dedicated Digital Identity System regulatory scheme through legislation (which would address all three problem areas).

The analysis presented in this Regulation Impact Statement (RIS) indicates that Option 3: Dedicated Legislation to Establish New Regulatory Scheme most

comprehensively addresses the identified problem areas, fulfils the policy objectives, and delivers the greatest overall net benefit. For this reason, it is the preferred approach. However, this Regulation Impact Statement (RIS) examines the relative costs and benefits of all potential options for achieving the stated policy objectives, via some form of legislation or use of regulatory frameworks.

This RIS has been developed to examine the case for establishing a dedicated regulatory scheme for the System, and to seek input on the likely regulatory impact of the proposed measures. Each of the seven RIS questions, and the applicable section/s of this document which address them, are set out in Table 1.

RIS question	Relevant document section
1 What is the policy problem you are trying to solve?	3 What is the problem?
2 Why is government action needed?	4 Requirement for government action
3 What policy options are you considering?	5 Policy options overview
4 What is the likely net benefit of each option?	6 Approach to determining costs and benefits of options 7 Likely net benefit of Option 1 – Status quo 8 Likely net benefit of Option 2 – Leverage existing regulatory frameworks 9 Likely net benefit of Option 3 – Dedicated regulatory scheme
5 Who did you consult and how did you incorporate their feedback?	10 Consultation to date and future roadmap
6 What is the best option from those you have considered?	11 Best option from those considered
7 How will you implement and evaluate your chosen option?	12 Implementation of selected option

Table 1: RIS questions and accompanying relevant document sections

2 Introduction

2.1 Purpose of this document

This document examines the case for regulating the System, including the relative costs and benefits of all viable options considered. It assesses the estimated regulatory impact of all options, with particular focus on the preferred option (Option 3: Dedicated legislation to establish new regulatory scheme).

This RIS is being publicly released with Exposure Drafts of the Trusted Digital Identity Bill, the Trusted Digital Identity Framework (TDIF) accreditation rules and the Trusted Digital Identity (TDI) rules (Exposure Draft package), as part of the Program's ongoing, broad-based consultation on regulation and other System-related matters. The release of this document alongside the Exposure Draft package provides further transparency on the government's decision-making process, and will enable regulatory impacts of measures under consideration to be tested with stakeholders.

Consultation questions

Specific questions on which input is sought, and categories of information requested, are set out in this document in Sections 7, 8 and 9, highlighted in blue boxes. In summary, the questions seek to:

- validate the accuracy of the regulatory impact assessment for each option
- give stakeholders the opportunity to provide further information on the existence or extent of potential impacts of proposed regulatory measures.

Input is sought on impacts of the proposed regulations only. This RIS is not seeking submissions on the suitability of the policy options considered, alternative approaches, or the content of the legislation or rules. These matters have been the subject of multiple rounds of consultation to date, and any further related submissions should be made in response to the broader Exposure Draft package (rather than this RIS). It is also not consulting on the operation of the System, the Trusted Digital Identity Framework or how government services are delivered generally.

Consistent with Australian Government guidelines, a final assessment RIS will be completed prior to a final policy decision (either the introduction of a Bill to Parliament, or a full policy announcement).

2.2 What is a Digital Identity?

A Digital Identity is a safe, secure and convenient way for Australians to prove who they are online. It only needs to be created once, then can be reused whenever a person is asked to prove online who they are when accessing a linked service. When rolled out across a variety of government entities and businesses, individuals can securely access connected services online. Digital identity also provides efficiencies for the public and private sector, giving small and medium enterprises more time to manage and grow their businesses.

While it can be reused once created, a Digital Identity is not a single, universal or mandatory number, or an online profile. Personal information remains private and protected. People must provide consent before their details are shared with the service they wish to access. A Digital Identity does not replace physical identification documents such as a birth certificate, visa or driver's licence. Australians who cannot or do not wish to use a Digital Identity can continue to access government and other services at shopfronts or over the phone. There are multiple identity proofing levels, offering different degrees of proofing rigor and identity confidence which can be used for differing purposes (and also can offer cost efficiencies, as lower standards of identity proofing require less information from the user and can be undertaken at lesser cost). Importantly, Australians will retain their choice to use a Digital Identity, must consent to each transaction, and will be able to close their account at any time they wish.

2.3 Australian Government Digital Identity System

2.3.1 Background

> Australia's current identity infrastructure is fragmented, consisting of a largely uncoordinated network of identity credentials. The System has developed organically, driven by different standards, policies, and legislative requirements.

(Source: Commonwealth Treasury 2014, *Financial System Inquiry*).

The 2014 Financial System Inquiry Report (Murray report) found that Australia's current identity environment is fragmented and uncoordinated. In the past, government entities have largely operated in siloes, developing bespoke identity initiatives to manage internal fraud risks or to deliver specific policy outcomes. As described in the Murray report, this has resulted in duplicated investment, wasted resources, a fragmented identity environment and poor customer experiences. People and businesses wanting to engage with government often do so at high cost, leading to frustration and reduced confidence in government. This has the potential to result in a reluctance to trust and use government digital services. The Murray report recommended a national identity strategy that would improve efficiency and security across the digital economy.

Through the Program, commenced in 2016, the Australian Government is working to deliver better outcomes for all Australians by making it easier for them to access the services they need. The Program is building a trusted System for the entire Australian economy, with the potential to transform the way people and businesses access services online. Already, significant progress has been made towards building a nationally consistent identity verification system, alleviating pain points, and closing the gap between the customer experience offered by government and the private sector. To date, the Digital Identity Program has delivered the core foundations for the platform and is currently used by over 3.3 million people and over 1.3 million businesses to access more than 77 digital Commonwealth services. (Source: Digital Transformation Agency 2021, *Objective 3 - You will be able to choose a secure and easy-to-use digital identity to access all digital government services.*)

2.3.2 System governance: Trusted Digital Identity Framework (TDIF)

The TDIF, developed in collaboration with key government entities, peak industry bodies, privacy commissioners and other key stakeholders, is the means by which the System is governed and protected. It mandates strict operational standards by defining a complete set of requirements, roles and operating responsibilities for participants, that establish a nationally consistent approach to accredit the System in Australia.

The TDIF is built around eight guiding principles: user centric, voluntary and transparent, service delivery focused, privacy enhancing, collaborative, interoperable,

adaptable, secure and resilient. These principles work to ensure that privacy and the security of personal information remain central to the System. An individual may have multiple Digital Identities, but the TDIF ensures consistency in how they are established and managed.

Accreditation and onboarding

Accreditation and onboarding are key concepts within the TDIF, ensuring that the System remains secure and trustworthy. Entities are accredited as one of the specific roles within the System (e.g. attribute provider or identity provider). The accreditation process is rigorous and involves undertaking various activities and providing documentation to the accreditor (i.e. the Interim Oversight Authority, discussed further below), third party evaluations and operational testing. Entities who are accredited may or may not also be 'onboarded' to the System, referring to establishment of the physical connection of the entity's system to the System. Onboarding may occur 'indirectly' in some cases (particularly for credential service providers, which may connect only to an identity provider).

The key roles within and related to the System are described further below in Section 2.3.3 Entities, interactions and incentives within the current System. In summary, roles in the ecosystem fall into the following primary categories:

- **user** – an individual seeking to use the System. Does not need to be accredited nor onboarded
- **onboarded accredited entities** – entities that are accredited and onboarded to the System. Roles which require accreditation are attribute provider (**AP**), credential service provider (**CSP**), identity exchange (**IDX**) and identity provider (**IDP**)
- **relying parties** (services) – rely upon verified information provided through the System to provide a digital service. Must be onboarded, but not accredited.

In addition to the above, entities may choose to be accredited under the TDIF but not onboarded to the System for a number of reasons, including to enhance the perceived assurance of their identity system (**accredited entities**). Once accredited or onboarded, entities need to continually demonstrate they meet their TDIF obligations as relevant to their particular role and prove this by undergoing annual assessments.

Interim Oversight Authority

The Interim Oversight Authority is responsible for the administration and oversight of the System. Its functions are shared by the DTA and Services Australia and are performed independently from their broader agency responsibilities. Effective governance is essential to the efficient operation of, and instilling public trust and confidence in, the System. Accordingly, the Interim Oversight Authority holds a broad range of powers established through the System Governance Agreement that enable it to carry out its governance and operational responsibilities. These responsibilities include:

- applicant accreditation and annual assessment
- approval of participants and management of the participant register
- on-boarding participants to the System
- monitoring participant compliance in accordance with the TDIF and operating rules
- inquiries, investigations and coordination (but not limited to) of System incidents, change and release, fraud and security events
- service level reporting and management
- suspension and termination of participants
- 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.

2.3.3 Entities, interactions and incentives within the current System

Figure 1 portrays the entities currently involved in the System and explains their interactions and likely incentives. A more detailed description of these for each type of entity can be found at Appendix B Detailed entities, interactions and incentives within the current System. These key entities are onboarded accredited entities (various types), relying parties, the Interim Oversight Authority, and users.

Accredited entities are accredited under the TDIF to fulfil particular roles within the System and can be conceptualised as the *providers* of the different components required to deliver the System. To achieve accreditation, these entities must undergo a series of rigorous evaluations across all aspects of their operations. This includes demonstrating how their service/s meet strict requirements for usability, accessibility, privacy protection, security, risk management, fraud control and more. Accredited roles include **IDX**, **AP**, **CSP** and **IDP.**

There are also key entities within the System which are not accredited under the TDIF. These are:

- **relying parties** – approved entities (including hubs and portals) providing online services to people with a digital identity. (Hubs and portals are relying parties that provide attributes to services downstream. Through a Hub, a user may be able to access multiple services or service brands, without linking. Through a portal, a user may be able to link and access multiple services or service brands)
- **Interim Oversight Authority** – the governing body for the System
- **users** – who create one or more digital identities and use these to access services via relying parties.

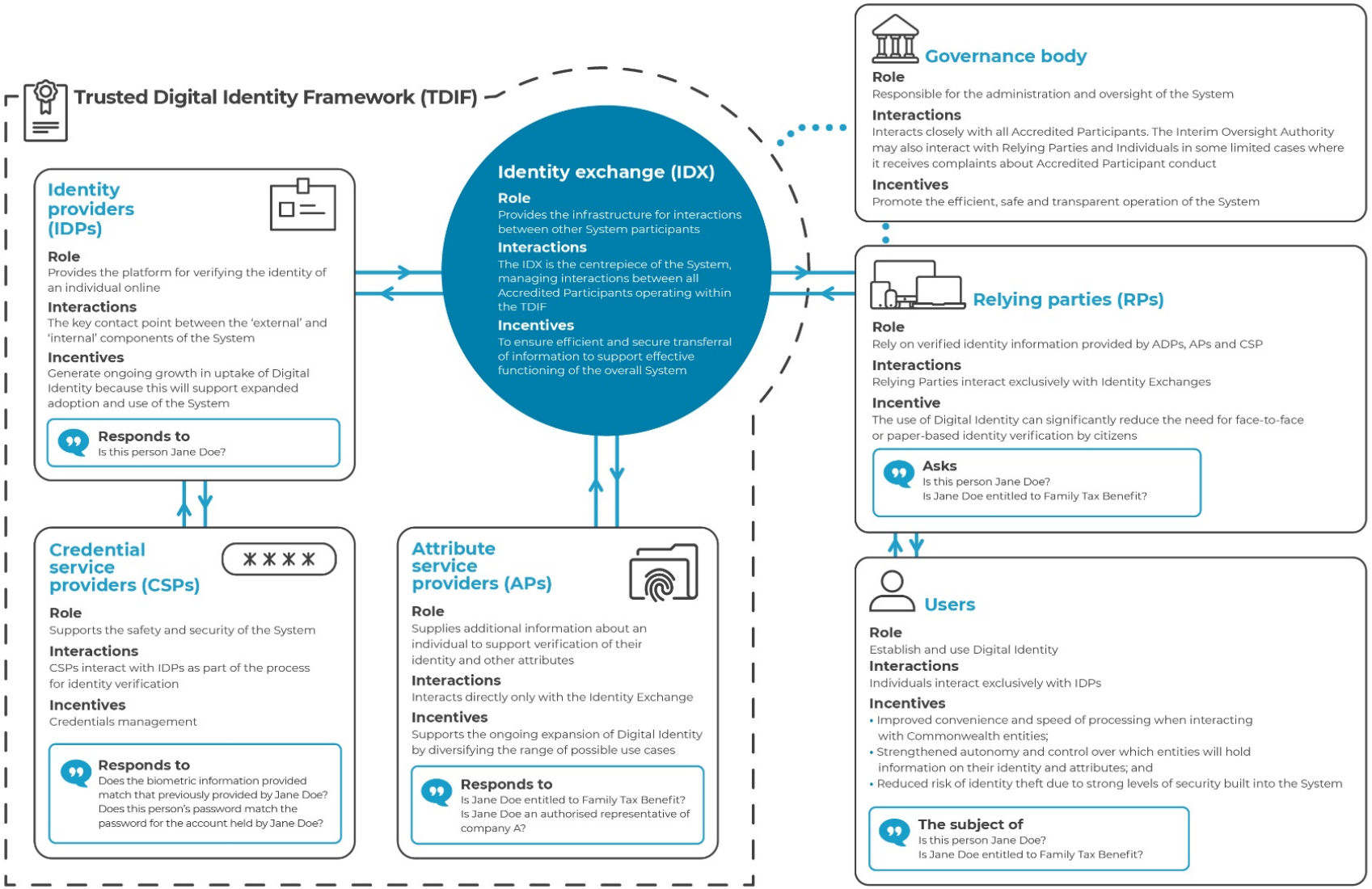


Figure 1: Entities, interactions and incentives within the current System

2.4 Benefits and value of the System

The System stands to assist individuals, businesses, government, and the overall economy in many different ways. The System's key benefits, which will also help to drive uptake, include:

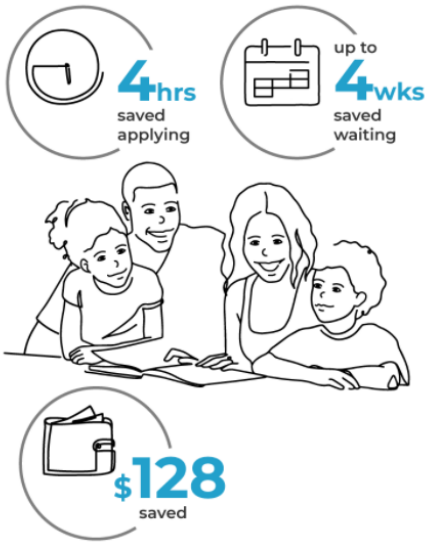
- For individuals (users):
  - improved speed of interaction with a wider range of Australian Government, state, territory and local government entities, as well as private sector businesses
  - greater choice and flexibility in interactions with identity providers, appealing to individuals' varying preferences
  - reduced risk of information or data loss and identity fraud, encouraging greater confidence in Digital Identity
  - strong levels of autonomy and control compared with other emerging 'de facto' identity solutions which are increasingly used to transact with private companies online.

The efficiencies and benefits available to individuals and families are illustrated by the below example.

Case study: Regional families affected by natural disaster

Henry is a farmer who has been reluctant to use online government services in the past, preferring to make an hour-long drive to visit a Services Australia service centre or an Australia Post shop front instead.

After battling extreme drought, Henry decides it is time to use government services online and create his Digital Identity so he can quickly set up new online accounts. He can



no longer afford to lose hours on the road when he needs to be on the farm.

When a bushfire tears through the family property and destroys his family's birth certificates and passports, Henry realises the value of his Digital Identity. With his Digital Identity, he doesn't need to wait for replacement documents and he can still access all of the government services he needs.

- For businesses:
  - time, cost savings and enhanced productivity, as a result of the increased speed of transacting with multiple government agencies or businesses
  - improved efficiency of customer operations and reduced manual handling
  - reduced instances of customer fraud, which is particularly beneficial for banking and financial service providers, as well as any entity with 'Know Your Customer' obligations. (Reporting entities under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) have obligations to apply customer identification procedures to all customers, and alter their procedures based upon the level of money-laundering/counter-terrorism financing risk that different customers pose)
  - provides the same means of accessing personal and business services saving time and effort
  - greater opportunities for growth in domestic markets, particularly in sectors such as financial technology (FinTech) and regulation technology (RegTech), and the broader Australian economy through realising the efficiencies above.

The efficiencies and benefits available to businesses and business owners are illustrated by the below example.

Case study: Starting a new business

Alex is an IT specialist who decides to fulfill his long-term ambition of starting his own small business. He wants to get his new business off the ground as quickly as possible, particularly because he is the primary earner in his family.

Alex has a number of steps to complete including applying for an ABN and registering his business name.

A former colleague urges Alex to try using Digital Identity. Alex finds the process takes a quarter of the time it otherwise would have, and he also saves $128 in avoided costs.

- For governments of all levels:
  - reduced time and demand for government services to verify an identity, and people may engage in end-to-end digital transactions further reducing transaction times
  - reduced need to maintain agency-specific identity and access management systems and associated support systems
  - increased security of people's information, reduction in the cost of fraud and improved detection, monitoring and response
  - improved integrity of service provision, contributing to improved user experience, knowledge and public trust.
- For the economy:
  - increased productivity with the use of the System and associated increased in digital service consumption, saving people and businesses time and money

- efficiency benefits flowing from the opportunity for financial institutions to reuse customer data stored in Digital Identity
- reduction in costs to the economy, linked to reduction in the rate of fraud and identity theft
- increased productivity as people and businesses can complete essential transactions with government and other organisations more quickly.

With a fundamental design principle of the System being that people, businesses and agencies choose to become a part of the System, a broad range of stakeholder expectations have been consistently considered to ensure the System provides a service that benefits all that use it.

2.5 The case for expanding the System

2.5.1 Benefits of expansion

Having delivered the foundational capability and infrastructure, the governing policy, the security and risk management framework, and underlying operational support, the Program received $256.6 million over two years in the 2020-21 Budget to expand the System. This expansion is focused on making the System available as a whole-of-economy solution, enabling all Australians and businesses to have more secure and convenient engagement with government (including state, territory and local) services and, in the future, the private sector (source: Ministers for the Department of Social Services 2020, *Delivering essential support and services through unprecedented times* media release). The improvements will deliver enhanced digital services experiences, particularly for small and medium businesses and individuals.

Further expansion of the System forms a critical part of government's Digital Business Plan – an investment of almost $800 million to enable businesses to take advantage of digital technologies to grow their businesses and create jobs. The System's value was clearly demonstrated during Australia's response to the COVID-19 pandemic, which has seen an unprecedented increase in the use of digital channels throughout the implementation of JobSeeker, JobKeeper and other stimulus measures. Rather than being a tactical solution designed to address the

immediate issues faced as a result of COVID-19, the System provides a more strategic and longer-term whole-of-economy solution.

While Digital Identity's value is ongoing, events such as the pandemic and the 2019-20 bushfires, have reinforced the critical role technology plays in enabling people and businesses to deliver and receive trusted services in times of crisis. As the Hon Stuart Robert MP observed in April 2021, "the expectations and needs from people and businesses have changed dramatically over the past 12 months, with the demand for digital services growing significantly". ABS data reinforces the expectation that increased demand for government services will continue, with small, medium and regional businesses in particular, urgently needing a safe and secure way to access critical services, payments and supports to assist their ongoing recovery. (The most recent ABS statistics indicate there are around 701,100 unemployed people as of January 2021, reflecting the ongoing impact of COVID-19. One in five (20%) businesses have stopped accessing at least one support measure (government or otherwise) since March 2021, but government support continues to be a factor that influences planned capital expenditure of businesses for the next three months (when asked in February 2021 and November 2020). Source: Australian Bureau of Statistics, Business Conditions and Sentiments (May 2021) and *Labour Force, Australia (*May 2021).) Similarly, people getting their first job or being re-hired, require quick access to services enabling this to occur as quickly as possible.

The expansion of the System also presents opportunities to modernise public services at a state, territory and local government level. The extent and frequency of individuals' touchpoints with state, territory and local government-provided services means the System – through its enablement of reduced paperwork, faster transactions and improved convenience – can generate significant gains in administrative efficiency. These benefits are expected to support state and territory government services, including the registration of births, deaths and marriages; licensing regimes; utilities; healthcare; and education. These levels of government would also realise the System's other benefits described above, including reduced identity fraud.

Further, research conducted by the World Economic Forum (WEF) suggests digital identity is essential for the growth of the digital economy more broadly. By

encouraging digital, as well as physical, engagement with public and private sector services, it has a pivotal role to play in rebooting the global economy in the aftermath of the COVID-19 pandemic and beyond. Digital identity uniquely positions businesses, the research concluded, to gain and maintain user trust and remain competitive, "… guarantee[ing] the realisation of greater economic potential…and advancing an economy that is more inclusive, equitable and stable for all" (source: *Shaping the Future of Digital Economy and New Value Creation* 2019).

2.5.2 Entities, interactions and incentives within an expanded System

Figure 2 portrays the entities that would be able to participate in an expanded Australian Government System, including their likely interactions and incentives. A more detailed description of these can be found at Appendix C: Detailed entities, interactions and incentives within an expanded system. One of the primary points of difference between the below and Section 2.3.3 Entities, interactions and incentives within the current System, is the inclusion of non-Commonwealth agencies as relying parties and the expansion of onboarded accredited entities that would be enabled by a legislative charging framework. Unless otherwise stated, the nature of the roles for each type of entity remain broadly the same.

Non-Commonwealth agencies can currently participate in the System as onboarded accredited entities, and as relying parties in a test (beta) capacity. However, as discussed below, they face reduced incentives to do so compared to under an expanded scheme, with a legislative charging framework. Under an expanded System, with appropriate statutory basis, non-Commonwealth agencies would be better incentivised to participate as onboarded accredited entities and legally enabled to participate as relying parties.

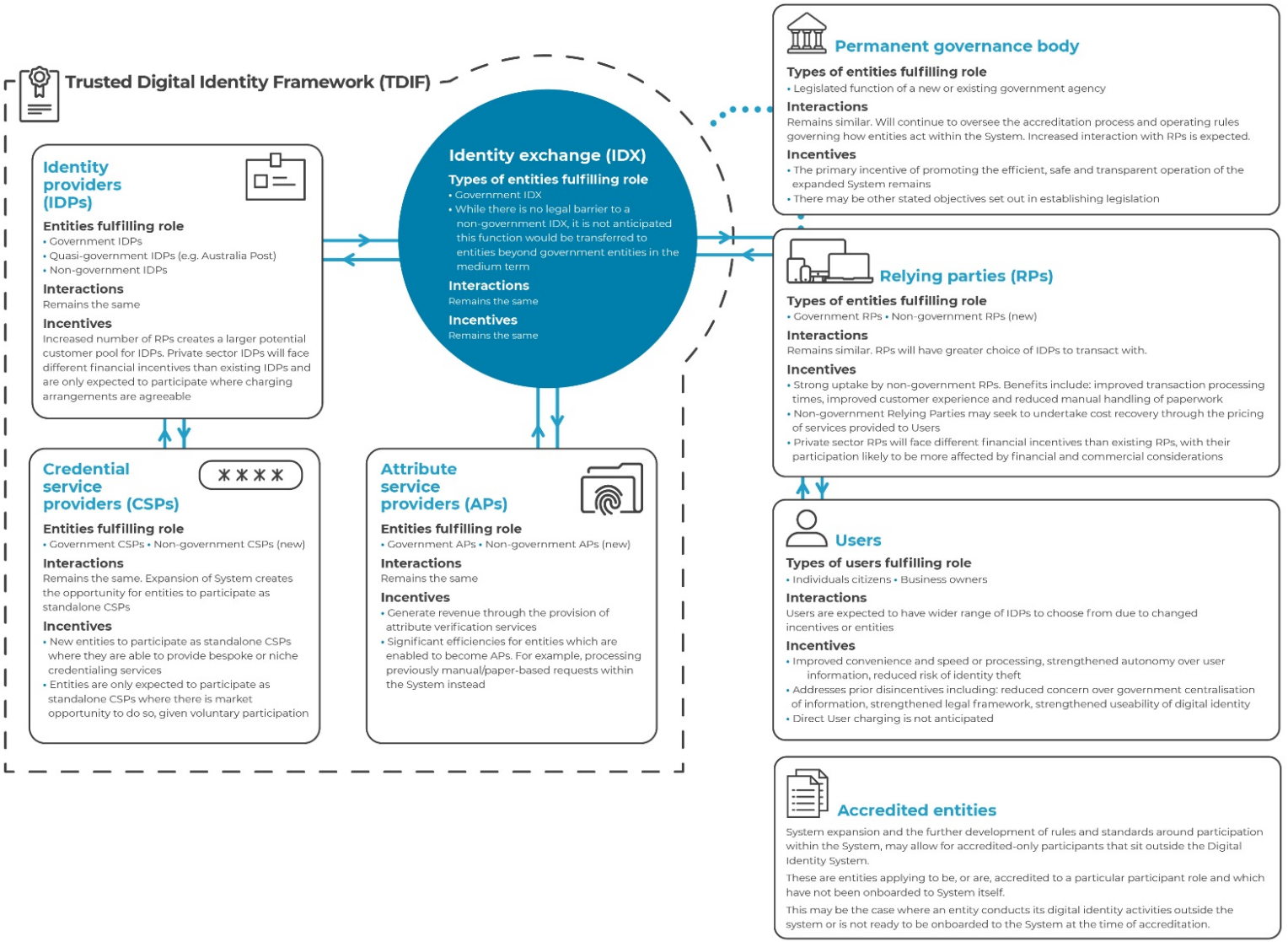


Figure 2: Entities, interactions and incentives within an expanded System

3 What is the problem?

3.1 The importance of a whole-of-economy solution with global application

The foundations of a trusted, nationally consistent System have been established. However, full realisation of its long-term benefits will only be achieved through adoption of the System across the economy, eventually connecting state, territory and private sector services as well as Australian Government ones. Successfully delivering the System's expansion will further change the way online verification occurs, unlock value across the broader economy, and transform service delivery across Australia. Legal and regulatory foundations play an important role in building strong governance for the System, and are essential in building confidence for the service providers connected and citizens choosing to use their Digital Identity.

Numerous studies have recognised the global potential of digital identity. McKinsey Global Institute's 2019 research paper 'Digital identification: A Key to Inclusive Growth' found that extending full digital identity coverage could unlock economic value equivalent to 3–13% of GDP in 2030, reduce institutional customer onboarding costs and payroll fraud, saving up to US$1.6 trillion globally, and save approximately 100 billion hours through streamlined e-government services. The WEF has estimated that 70% of new value created in the economy over the next decade is expected to be delivered by digitally-enabled platforms. Conversely, it estimates that the ongoing absence of a cohesive and secure digital identity solution, available in both public and private sector contexts, will present a block to economic growth – with businesses already losing up to 30% of potential revenue due to inefficiencies and poor user experience (source: *Reimagining Digital Identity* 2020, World Economic Forum).

The benefits of expanding the System across the broader Australian economy in particular have also been quantified in various research papers, which indicate the potential realisation of significant economic value. Australia Post's 2016 paper 'A Frictionless Future for Identity Management' shows that extending full System coverage across Australia, by addressing current gaps, has the potential to realise up to $11 billion per annum through reduced cost to serve, cost of fraud and improved customer experience. Economic analysis conducted by KPMG found that

full uptake of Digital Identity, scaled up by just three cohorts within the Australian economy (new businesses, apprentices, and domestic university students), has the potential to generate time savings worth as much as $368.3 million over five years and reduce identity crime, which is estimated to have an annual cost of over $2 billion.

Research has also identified those sectors of the domestic economy which would particularly benefit from a full expansion of System capability. For example, enabling private sector participation in the System would expand local opportunities for Australian RegTech and FinTech businesses, supporting growth of a homegrown market and economy. In 2020, Australia had the third-highest number of RegTech companies globally, with more than 80 RegTech companies headquartered in the country. However, a recent study by BCG and The RegTech Association found that this strong position is under threat, with investment in local RegTech declining 50% since 2018, whilst a corresponding increase to record investment levels has occurred globally. Research from BCG and The RegTech Association highlights regulatory reform as critical to addressing this trend, identifying that such enhancements to regulatory and policy frameworks must 'encourage innovation'. The System provides an opportunity for government to invest in a whole-of-economy business tool, which can contribute to retention and development of a vibrant Australian RegTech sector, whilst supporting the export of Australian solutions into overseas markets.

With global spending on RegTech expected to more than double by 2025 to USD $50–$75 billion, this is an area of pronounced opportunity for growth in the Australian economy and the creation of new jobs (source: Parliament of Australia 2020, *Submission to the Senate Select Committee for Financial Technology and Regulatory Technology*). RegTech firm HooYu reported in 2016, "with 61% of individuals surveyed saying they would not trust other parties in a peer-to-peer transaction, good digital identity will enable the creation of new marketplaces and business models based on trusted interactions, and through them, new revenue streams".

Additionally, FinTech businesses also stand to benefit from an expansion in the availability and uptake of Digital Identity. Where FinTech companies seek to capitalise on digital identity solutions, Australians' traditional interactions with

financial and banking services can be improved (source: Stellar, D 2021, *Digital identity the next frontier for FinTech innovation*). Digital Identity's capability to capture historical interactions with FinTech entities and profile spending habits, while ensuring the security of personal information, will allow for efficiency gains across banking and financial transactions. Beyond this, FinTech entities will be afforded the opportunity to improve their products and present Digital Identity as a service offering, transforming traditional banking and financial business models (source: Contri, B and Galaski, R 2016, *Picture perfect: A blueprint for digital identity*).

3.2 Potential barriers to realising whole-of-economy benefits

There are several barriers which have the potential to impact the System's expansion across the Australian economy, and the full realisation of benefits described above. These are:

- No legal basis for participation on non-Australian Government entities, nor for a charging framework
- Lack of trust in the System's privacy and security safeguards
- Interim, non-legislative governance framework.

3.2.1 No legal basis for participation of non-Australian Government agencies as relying parties, nor for a charging framework

The eventual participation of non-Australian Government agencies, such as state, territory and local governments, private sector and community organisations, and foreign governments, is critical to unlocking the System's whole-of-economy value. While non-Australian Government agencies can currently become onboarded accredited entities (for example, Australia Post's Digital iD solution – which is accredited but not on-boarded), legislative authority is required to include non-Australian Government agencies as relying parties (except in limited circumstances).

Without the legal authority for participation of these entities as relying parties, the System could be used to transact with Australian Government agency services only. This represents a missed opportunity for the Australian economy as it would deprive the private sector and a large share of the public sector of the System's efficiency

benefits and limit the growth and innovation of industry segments such as FinTech and RegTech. It would also not address the Murray report's conclusion that a whole of economy solution is necessary, where public and private sector identity providers compete to supply trusted digital identities to individuals and businesses.

Additionally, there is currently no legal basis for a charging framework to be established for the System. The absence of a permanent, transparent, consistent charging framework limits the incentives for non-Australian Government agencies to become onboarded accredited entities. Unlike relying parties above, there is no legal impediment to non-Australian Government agencies choosing to become accredited and deliver services within the System. However, from a practical perspective, it is not expected that non-Australian Government agencies would be adequately incentivised to do so, without a charging framework underpinned by legislation.

This problem presents a fundamental obstacle to System expansion, and therefore impacts a broad range of stakeholders who would potentially benefit from such expansion including current and potential System participants, relying parties and users. It also has a broader impact on the economy and community at large, due to the foregone benefits of an expanded system.

3.2.2 Lack of trust in System's privacy and security safeguards

The System has been designed and built with a central focus on privacy, security and consumer protection. Notwithstanding this, an expanded System may render certain aspects of privacy and security more difficult to enforce if not backed by legislation, with potential adverse impacts upon the level of trust and confidence Australians have in the System.

Privacy and security by design

The System is designed to ensure the privacy of individuals is protected and strong safeguards are in place to protect data and personal information. While using Digital Identity, personal information is securely encrypted and protected by strict Australian Government security protocols. Additionally, the TDIF framework governing use of the System currently includes a range of System-specific privacy and consumer protections for individuals. These 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.

Onboarded accredited entities are bound to comply with these requirements, which are established by the Interim Oversight Authority. A breach may result in a participant losing its accreditation status. However, the TDIF is not law, and the Interim Oversight Authority has no legal or regulatory enforcement powers outside the established governance arrangements. As a result, the Interim Oversight Authority has limited ability to enforce System requirements unless they are also contained in other applicable legislation or regulations. This is a manageable state of affairs when all System participants are Australian Government entities, but is not sustainable if the System were to expand to encompass other participants.

Existing privacy safeguards

This existing framework of legal and other requirements, which also may apply to the activities of onboarded accredited entities, includes the *Privacy Act 1988* (Cth) (Privacy Act), Australian Privacy Principles and the Privacy Code, Information Security Registered Assessors Program, Australian Government Protective Security Policy Framework and Information Security Manual and Australian Signals Directorate's Essential Eight cyber security mitigations.

The Privacy Act is Australia's principal piece of legislation for the protection of personal information, including its handling, collection, use, storage and disclosures (source: Commonwealth Attorney-General's Department 2021, *Privacy)*. There are various circumstances in which an entity may be excluded from compliance with the Privacy Act. For example, in many cases, the acts and practices of state and territory agencies, private individuals, universities, and small business operators are not covered by the Privacy Act (source: Office of the Australian Information Commissioner 2021, *Rights and responsibilities)*. In the absence of System-specific legislative requirements, the legal obligations applying to a Participant's activities within the System are dependent upon whether or not they are bound by the Privacy Act.

Currently, where an entity is captured by the Privacy Act's provisions, the Notifiable Data Breaches Scheme (NDB Scheme) mandates reporting to both the affected

person/s and the Office of the Australian Information Commissioner (OAIC), when a data breach occurs. However, if an entity is exempt from or has only security obligations under the Privacy Act (such as a small business operator's obligation to secure Tax File Number information), such reporting requirements will not apply (source: Office of the Australian Commissioner 2019, *Part 4: Notifiable Data Breaches Scheme*).

The OAIC is the national privacy regulator, responsible for upholding Australia's privacy legislation and initiatives. The OAIC is allocated various powers and responsibilities under the *Australian Information Commissioner Act 2010* (Cth) ('AIC Act'), including investigating potential acts or practices which breach privacy legislation, conducting privacy assessments on entities' handling of personal information, and compelling entities to develop enforceable privacy codes (source: Office of the Australian Commissioner 2021, *What we do*).

Potential inconsistencies in legal obligations applying to participants

Whilst the above privacy and security protections have provided appropriate coverage for the System's limited use and participants to date, expansion to non-Australian Government agencies may result in inconsistent legal coverage. Expanding to a whole-of-economy System under existing privacy and security settings, may surface the below potential gaps across Australian Government, state and territory level legislation:

- individuals may not be able to seek redress about the actions or practices of Identity IDPs, IDXs and APs involved in the System that breach the Privacy Act, where onboarded accredited entities are state or territory agencies
- Australian Government agencies must conduct Privacy Impact Assessments (PIAs) for high privacy risk projects under the Australian Government Agencies Privacy Code and Privacy Act. This identifies a project's impact on the privacy of individuals and ensures that they have a plan in place to safeguard it. However, this is not an explicit requirement for private sector organisations covered by the Privacy Act, nor for organisations not covered by the Act
- legislative penalties and sanctions for prohibited disclosure of sensitive and other personal information currently apply to participants as a result of the Privacy Act. However, the Act currently only applies to 'APP entities' – primarily Australian Government entities and private sector organisations with a turnover

of more than $3 million. Under these arrangements, there would be no legal recourse for breach of the Privacy Act by an onboarded accredited entity that is a small business or start-up with less than $3 million turnover, nor a state or territory agency.

The interaction between Australian Government, state and territory privacy laws is particularly important to provide a uniform level of protection for information used in connection with the System. Privacy legislation operates in most states and territories. However, even for jurisdictions without privacy legislation, there are common guidance documents and non-binding policies which seek to regulate the approach to privacy. These requirements and enforcement mechanisms vary across jurisdictions to varying degrees. To instil confidence and trust amongst individuals and prospective System participants, it is preferable that privacy protections apply as uniformly as possible.

This problem area particularly impacts individuals impacted by a data breach or misuse of their personal information through, for example, not being able to seek redress from the OAIC. Apparent inconsistencies in privacy protection (potentially affected by variables such as onboarded accredited entity type and jurisdiction) also impacts broader community confidence in the System with potential impacts on uptake, as discussed further below.

Instilling greater trust through consistent safeguards

The importance of strong, consistent privacy and security safeguards was highlighted in September 2018, by the System's second PIA. Consulting with stakeholders, this assessment reported a strong prevailing view that a single set of legally enforceable rules would provide participants with consistency, and the broader Australian community with trust and confidence in using the System. Of particular significance, it noted, was the fact that incorporating key privacy protections into legislation or a legislative instrument would ensure "they cannot be removed or weakened without scrutiny".

There is evidence to indicate that, at a community-wide level, Australian attitudes and views about privacy are rapidly evolving. Research shows the increasing importance of data security to individuals and potential participants in the System, with protection of personal information cited as a paramount consideration in

business' and individual's digital activities (source: *Digital Identification: A key to inclusive growth* 2019, McKinsey Global Institute). Recent polling by the OAIC has found that 97% of Australians consider privacy important when choosing a digital service and 87% of Australians want more control and choice over the collection and use of their personal information. A majority (66%) of Australians were found to be reluctant to provide biometric information to a business, organisation or government agency (source: Office of the Australian Information Commissioner 2020, *Australian Community Attitudes to Privacy Survey 2020*). This wariness is not limited to potential commercialisation of personal data. OAIC's survey also found that only 36% of Australians are comfortable with their personal information being shared between government entities, and only 13% are comfortable with businesses sharing their information with other organisations (source: Office of the Australian Information Commissioner 2020, *Australian Community Attitudes to Privacy Survey 2020*).

This increasing level of concern is driven, in part, by the growing prevalence of identity crime, which is now one of the most common forms of criminal activity in Australia and was estimated to cost $3.1 billion (including direct and indirect costs) in 2018–19 (source: Franks, C & Smith R 2020, *Identity crime and misuse in Australia: Results of the 2019 online survey Statistical Report no. 27)*. The risk posed by this criminal behaviour has only increased during the COVID-19 pandemic, with figures released from the Australian Consumer and Competition (ACCC) in August 2020 showing identity theft up 55% on the same period in 2019. In this context, Australia's growing concern with privacy and the security of personal data could significantly impact the uptake of Digital Identity, which requires sharing of personal data, including biometrics. (Internal DTA Program research has validated the high priority that individuals place on 1. Reassurance that their information is safe and secure, and 2. Proactive security monitoring.) If the System is to retain public trust whilst it expands across the economy, enabling the realisation of whole-of-economy benefits, public concerns over data privacy and security need to be decisively and permanently addressed.

3.2.3 Interim, non-legislative governance framework

Effective governance of the System is essential for its efficient operation, to instil public trust and confidence and promote individual uptake. While the interim governance structure has proven effective to date, there is a risk that the current

arrangements may not sufficiently enable the System to expand beyond non-Australian Government agencies, while maintaining high standards of integrity.

What could be improved in the current governance framework?

The interim arrangements have, to date, proven to be an effective governance model. However, an expansion of the System is likely to encourage greater participation from private sector onboarded accredited entities and, for the first time, support the participation of non-Australian Government relying parties. Without making corresponding amendments to the System's current governance framework, greater participation in the System could result in several problems occurring, as described below:

- **Certainty** – the current governance arrangements are interim and not underpinned by legislation. The absence of an established, permanent structure to govern the System may lead potential non-Australian Government participants (in their capacity as onboarded accredited entities or relying parties) to doubt its long-term viability, and therefore impair uptake
- **Enforceability** – the System Governance Agreement, which sets the role and powers of the Interim Oversight Authority, provides contractual and policy powers, but not regulatory ones. Specifically, the Interim Oversight Authority does not have the regulatory power to:
  - where justified, initiate enforcement action against participants to ensure rules are upheld and breaches addressed
  - take certain investigatory actions, such as compelling or directing participants to undertake an action or provide certain information in the course of making inquiries and undertaking investigations into the activities of participants
  - administer charging for authentication, to varying degrees of identity proofing, once the System is sufficiently mature
  - impose civil penalties.
- **Transparency** – as the arrangements governing the Interim Oversight Authority are not publicly accessible, they are not as transparent as having a permanent Oversight Authority, with a legislated role. While TDIF rules do currently require some transparency measures for onboarded accredited

entities (e.g. that IDXs publish Annual Transparency Reports), a permanent governance authority could also enforce and comply with publicly accessible legislative provisions and rules that are put in place to ensure transparency in the operation of the System

- **Independence** – the Interim Oversight Authority is structurally independent from other participants in the System, but comprises officials from two Australian Government agencies who have policy and operational roles. To ensure trust in the System and its governance model as expansion occurs, it is important that independence of the oversight body increases commensurately with the scale of the System in a way that makes it independent from other government functions and entities participating. The independence of the Interim Oversight Authority is also not clearly entrenched within and guaranteed by law, which may impact public trust in the governance integrity of the System as it expands beyond Australian Government agencies
- **Accountability** – while the System Governance Agreement imposes reporting requirements on participants and the Digital Identity Program reports to Parliament (e.g. through Senate Estimates), the oversight body would benefit from clear, legislated lines of public and Parliamentary accountability specifically tailored to the System, as well as any additional reporting requirements considered suitable (such as periodic and ad hoc reporting).

This presents an opportunity to improve governance for a broad range of stakeholders, including current participants, operating under non-legally enforceable rules, and future participants, by increasing their incentive to join the System. The impact of not having a trusted, robust governance framework is described further below.

Impact of not having a trusted, robust governance framework

The importance of a strong, trusted and independent governance framework has been recognised since before the commencement of the Program. The 2014 Murray report specifically identified fragmented governance arrangements as a contributor to the initial digital identity problem, observing that “although government has some existing governance mechanisms, the lack of clear ownership of identity policy is impeding progress”. There is a risk that an interim governance framework, whilst

appropriate to cover the System's limited participants and activities to date, may not meet community and prospective participant expectations for its future expansion.

Confidence in the robustness of governance mechanisms is equally important as having privacy, security and consumer protections. Governance is relied upon to put mechanisms in place to ensure compliance with the System's rules and take enforcement action when breaches occur. Without a strong governance framework there is heightened risk that the System will not operate as intended, resulting in potential low levels of public trust and a resultant reduction in uptake of the System and online services. The WEF has also recognised this, noting that:

> Strong governance and transparency of the data and business models behind digital identity provision are key to build trust with people. To avoid surveillance, the safe capture, storage, transfer and agreed usage of identity data requires strict oversight.

The Program's achievement of whole-of-economy outcomes, stimulation of innovation and economic development is reliant upon broad participation in the System – from individuals, onboarded accredited entities and relying parties, among other key actors. Expanding the System without making corresponding amendments to strengthen its governance framework could jeopardise this participation. A permanent Oversight Authority, maintaining and establishing a set of operating rules, would provide a greater level of certainty to all participants. This certainty is essential in persuading prospective participants in the System to make the required investments and participate.

Stakeholder consultation conducted to date has reinforced the importance of a robust governance framework entrenched, ideally, through legislation. During the PIA process conducted into the System in 2016, numerous stakeholders raised concerns about the lack of underlying legal authority for the establishment of the TDIF. The PIA observed that:

> It is possible the low expectations of success for the TDIF accreditation/revocation proposal are linked to the absence of any legislative basis or national agreement (such as Council of Australian Governments (COAG) directive) for the TDIF. If stakeholders could see a firm commitment backed by powers in legislation, some of the doubts regarding enforcement may lessen.

Since the 2016 PIA, progress has been made between states, territories and the Australian Government towards establishing a National Digital Identity Roadmap, one of the aims being an understanding on the customer experience across the range of potential digital identity systems and what will be needed from a governance and oversight perspective to ensure the systems and any customer transactions are proactively managed and from a customer-focused perspective. However, stakeholder views on the absence of legislation remain relevant. To address this issue, government regulatory action would need to establish a permanent, clear and nationally-applicable legal framework for the System which applies consistently across all potential future participants – including Australian Government, state, territory governments, private sector and community entities.

4 Requirement for government action

4.1 Government's role in delivering Digital Identity

The Australian Government has already taken a leading role in digital transformation, as articulated in its Digital Transformation Strategy (DTS). The Strategy aims to implement three key priorities: create a government that is easy to deal with, informed by the Australian people, and fit for the digital age. These priorities are further detailed through a series of 13 objectives, including a commitment that Australians "… will be able to choose a secure and easy-to-use Digital Identity [System] to access all digital government services".

The leading role taken by the Australian Government in delivering the System is legitimate, as government is best-placed to facilitate public-private sector collaboration in this area. The Murray report observed that previous industry-only attempts to manage and innovate on issues of identity have shown little success, and cited digital identity as:

> …a significant current example of an area where network benefits can be harnessed more effectively through public-private sector collaboration, and government facilitating industry action.

Importantly, the Murray report did not recommend government action at the exclusion of the private sector. Rather, it recommended that government intervention should focus on facilitating industry action and enabling private-public sector collaboration, through the right policy settings and risk-based regulation. (Currently, the public-private model has seen widespread adoption by both end-users and commercial providers in the international market, with the United States' and United Kingdoms' respective government-led Digital Identity initiatives, NSTIC and GOV.UK, proving to be exemplar programs. Source: Pon, B, Locke, C & Steinberg, T 2016, *Private-Sector Digital Identity in Emerging Markets*.)

Governments can also lead and coordinate investment in the underlying infrastructure, systems and processes which enable an effective national approach to digital identity, as the Australian Government has done in recent years.

In addition, the inherent sensitivities surrounding the collection of data and personal information, have led many to conclude that governments, rather than the private

sector, are best placed to manage and mitigate these concerns. For example, the McKinsey Digital Identification Report focused upon the importance of government action, in its capacity as a regulator and policy maker, for the development of policies and legal frameworks that enable acceptance of digital identity technology, while prioritising the protection of individuals' privacy.

4.2 Government's regulatory role and capacity

Having delivered the System, it is reasonable for the community, businesses and other actual and prospective users to expect that the Australian Government regulates and controls it. In relation to the problem areas of legal authority for expansion, privacy and security safeguards and governance, it is not appropriate for the Government to step back and allow 'the market' to deal with this. In this instance, the Government has created the market (noting that there are other private markets also currently operating in Australia) and therefore, should appropriately ensure it operates in a manner that enables the full, whole-of-economy benefits of the System to be realised.

The Australian Government also has the capacity to intervene successfully. Given the leading role it has played to date in delivering Digital Identity, and the regulatory options it has available, the Government is well positioned to ensure any System expansion meets the expectations of all Australians and promotes confidence in its integrity. Research from McKinsey concluded that governments are well-placed to address both the technical and legal components of Digital Identity, while ensuring accessibility and positive user experiences for all citizens. Comparable international examples where governments have introduced digital identity regulation further demonstrate the viability of government intervention in this space. (For example, in Denmark, the issuance, revocation and suspension of 'NemID' is regulated by two legislative instruments. In Finland, 'FINeID' is administered by the government's Population Register Centre and regulated through a special, specific legislative scheme. The United Kingdom's Department for Digital, Culture, Media and Sport has shared plans for a UK digital identity and 'attributes trust framework' including the introduction of a new legal framework.)

As identified, the government's Digital Economy Strategy cites the use of the System to access government services as a key objective. This alignment suggests

government intervention has already commenced and can be sustained and enhanced to support System expansion.

4.3 Objectives for government intervention

There are several specific objectives for government action, aligned with the identified problem areas. These are outlined in Table 2:

	Identified problem area	Objectives for government action
1	No legal basis for participation of non-Australian Government agencies as relying parties, nor for a charging framework.	Government action enables expansion of the System to include non-Australian Government agencies as relying parties, and providing a legal basis for charging by onboarded accredited entities (Australian Government and non-Australian Government), maximising the benefits.
2	Inconsistent privacy and security safeguards may become increasingly problematic as the System expands.	Government action enhances community confidence, trust and clarity regarding the Program's privacy and security safeguards.
3	Interim, non-legislative governance framework not sufficiently robust.	Government action to elevate existing protections into regulation enhances community confidence, trust and clarity in the integrity, permanence and rigor of the System's governance.

Table 2: Objectives for Government action

In addition to the above, it is expected that any government intervention will maintain or enhance the principles upon which the System is based. These are:

- **Choice** – ensuring that creation and use of a digital identity is voluntary at whatever Identity Proofing Level a person chooses to have, and that individuals also have the option to select from multiple identity providers
- **Consent** – requiring consent at multiple occasions when an individual interacts with the System, and the ability for that individual to withdraw consent at any time through an easily-understood process
- **Privacy** – safeguarding the personal information of individuals is the single most important design feature of the System, with privacy-enhancing principles embedded in its design and architecture

- **Security** – including specific security requirements which participants must comply with to become and remain accredited, and otherwise embedding security protocols in the System design
- **Integrity** – ensuring that an appropriate governance structure is in place, with an Oversight Authority responsible for operational System assurance, as well as safety, reliability and efficient operation of the System.

Considering these objectives for government intervention, a number of policy options have been formulated, discussed below in Section 5 Policy options overview.

4.4 Constraints and barriers to government intervention

Any potential government intervention must be undertaken with an awareness of constraints and barriers (either actual or potential). An inherent constraint upon any government action in digital identity is the complexity of this subject matter and the low familiarity and exposure of the community to this concept and the System to date. This apparent low level of public understanding of the System could lead to any Australian Government regulation in this area to be misconstrued or viewed with hesitation and distrust.

Research confirms that fewer than one in four Australians have a strong understanding of digital identity. This is validated by internal research undertaken by the DTA. In February 2019, a 12-month assessment of user insights found that most individuals did not understand the concept or value of digital identity and were seeking more information regarding learning and trusting the System itself. More recent public consultation undertaken has also elicited expectations including that the Australian Government "take advantage of lessons learned from earlier 'trust the government' initiatives with the proposed Digital Identity System legislation" (source: Digital Transformation Agency 2020, *Submission by the Northern Territory Government*) and that "government … must take responsibility for the impact and accuracy of their Systems" (source: Digital Transformation Agency 2020, *Submission by the Access Now*).

This low level of understanding and public confidence may also stem from previous Australian Government activity in national multi-use identity schemes (source: Hanson, F 2018, *Preventing another Australia Card fail*). As the New Payments

Platform chairman Bob McKinnon observed in 2019, the System stands at risk "of getting tied up to a whole lot of politics around what used to be the Australia Card", as well as other projects of a similar nature that were not ultimately pursued, such as the 2006-7 Access Card initiative. (See, for example, Bajkowski, J 2019, *How NPP chairman Bob McKinnon beats banktech delaying tactics*), and Jordan, R 2010, *Identity cards and the Access Card.*)

Successful regulatory intervention in this area will depend on clear and strategic communication to the broader Australian community on exactly what digital identity is and is not. Under the System, digital identity is not a single, universal or mandatory number, nor an online profile, and it will be important that this distinction is consistently conveyed. The Program has recognised this issue and has embedded this messaging within its public and stakeholder engagement efforts to date. As described further in Section 10 Consultation to date and future roadmap, future engagement will continue to address this misconception specifically as it relates to regulatory action.

4.5 Potential alternatives to government action

Alternatives to government action are considered in Section 5, namely within the 'status quo' option. This alternative would not support the System's expansion to non-Australian Government relying parties and legislatively enable charging by onboarded accredited entities, and would not address the privacy, security, and governance problem areas identified in this document.

5 Policy options overview

Three options have been considered in response to the identified problems:

- **Option 1** – Maintain the status quo
- **Option 2** – Leverage existing legislative frameworks to enhance privacy safeguards
- **Option 3** – Dedicated legislation to establish a new regulatory scheme for Digital Identity, enabling its expansion, entrenching privacy and other consumer protections, and establishing permanent governance arrangements.

Each option is described below, including applicable implementation considerations.

5.1 Option 1: Status quo

As Option 1 involves no regulatory action, it would see the existing System entities, interactions and incentives described in Section 2.3.3 Entities, interactions and incentives within the current System continue. This would entail ongoing application of TDIF policy to onboarded accredited entities and continued oversight by an interim governance body. The System would remain fully accessible by Australian Government relying parties only, with involvement continuing to be managed through System Governance Agreements/MoUs between Australian Government agencies. Onboarded accredited entities using the System would continue to be subject to existing legislative requirements which apply to them, including the Privacy Act.

Under the status quo, individuals can currently use the System through an identity provider: the Australian Government identity solution, myGovID. Individuals can continue to transact in the System with a select range of Government services and entities. As described above, it is not legally permitted for non-Australian Government agencies – including businesses or community organisations – to become fully operational relying parties (except in limited circumstances). Nor is there a legislative framework for charging within the System outside the Australian Government, practically limiting the incentives for non-Australian Government agencies to become onboarded accredited entities.

Under the status quo option, no discrete implementation activity would be required from the Australian Government. However, it would be expected that the Government would continue to serve its existing role leading the System's delivery. That is, continue to provide System oversight, make incremental adjustments as needed to the TDIF governance framework, and manage the entry of new participants. The entry of non-Australian Government participants, and further expansion of the System, would be limited by the absence of legislative authority for non-Australian Government relying parties and charging by onboarded accredited entities.

5.2 Option 2: Leverage existing legislative frameworks to enhance privacy safeguards

Option 2 involves leveraging existing regulatory frameworks to issue new instruments which address, to the greatest extent possible, the identified problems. The specific existing legislative framework which has been explored under this option are enforceable Registered Codes issued under the Privacy Act. While subordinate to primary legislation, Registered Codes are legally binding and will impose additional regulatory measures, including a bespoke enforcement regime.

Under this option, private individuals would continue to be able to use the services offered by identity providers and other onboarded accredited entities operating within the System. Participating entities would be accountable to a designated entity – such as the OAIC or a nominated Code administrator.

Part IIIB of the Privacy Act allows the Information Commissioner to approve and register enforceable Codes developed by entities on their own initiative, on request by the Information Commissioner or by the Commissioner directly. A Code developed for the System would operate in addition to the requirements of the Privacy Act, and could address some of the shortcomings described in Section 3.2.2 Lack of trust in system's privacy and security safeguards as well as providing an enforcement regime. As Codes under the Privacy Act are disallowable legislative instruments, this approach may address, to a certain extent, the identified problems relating to scrutiny and transparency of System privacy rules and requirements.

As it leverages existing regulatory arrangements, Option 2 would not be capable of providing legal authority for expansion of the System to private sector relying parties, implement a charging framework, nor establishing a permanent Oversight Authority. Therefore, it would see a continuation of the current governance arrangement, featuring joint oversight by Services Australia and the DTA, unless an alternative non-permanent, non-legislated governance arrangement is made.

5.3 Option 3: Dedicated legislation to establish new regulatory scheme

Option 3 involves establishment of a dedicated regulatory scheme for the System through primary and subordinate legislation. This would support an expansion of the System, by providing both the legislative authority to involve non-Australian Government relying parties, and the ability for onboarded accredited entities to be subject to a legislated charging framework. In addition to other measures described below, this new regulatory scheme would only apply to the Government's System (not digital identity systems in general, though other digital identity systems may choose to join the Government's System) and would ensure that it remains voluntary. Should individuals choose to participate, they will be able to select from a wider range of onboarded accredited entities (to whom the System would be more commercially attractive, with the ability to charge) and relying parties, beyond the current pool of Australian Government-only entities.

5.3.1 Key elements of dedicated regulatory scheme

Key measures proposed to be included in the regulatory scheme, which align with and address the identified problem areas, are listed below. As described in Section 10 Consultation to date and future roadmap, the Australian Government's position on each of these areas has been informed by ongoing analysis and consultation inside and outside the Government, continuing with release of the Exposure Draft package.

Application of regulatory scheme

Under this Option 3, legislation would enable Australian Government, state and territory entities (including local governments) and private entities to connect to the System to offer or use digital identity services in accordance with embedded privacy

and security safeguards. It would not apply to digital identities in Australia generally and would ensure that use of the government System remains voluntary. Additionally, in most circumstances (such as where restricted attributes are not involved) the scheme would not regulate services provided by a relying party in reliance upon a digital identity – regulation stops once the relying party has received verification of the person's digital identity.

The Bill's provisions apply primarily to the activities of onboarded accredited entities, relying parties and accredited entities, with regulatory powers and authority granted to the Oversight Authority and OAIC. The extent to which regulatory requirements apply is dependent upon what is appropriate given the particular role and interactions of the entity. For example, the integrity requirements dealing mainly with privacy obligations will not apply to relying parties (unless otherwise stated). This is because relying parties represent a low risk by obtaining limited information through the System, usually only the 'core attributes' for a digital identity.

Features of regulatory scheme

As set out in the Exposure Draft package, it is proposed that under this dedicated regulatory scheme, the System's implementation and operation would become a legislated function of a new or existing Australian Government agency. (This may be similar to the approach taken in 2009, when the *Personal Property Securities Act* created an office within the Australian Financial Security Authority (in the Commonwealth Attorney-General's Department portfolio), known as the Personal Properties Securities Registrar.) Once enacted, the new regulatory scheme would impose its own enforcement regime, including in some cases civil penalties for breaches of requirements. It would also cover the following:

- a legislative definition of digital identity (the set of information about attributes of a user which, taken together, allow an individual to be distinguished from another person), recognising that a person may have more than one digital identity. (Where the term "digital identity" is used in the context of the proposed Exposure Draft package and Option 3 (specifically, this Section 5.3 and Section 9), it can be assumed that this refers to the term as defined in legislation. In other sections of the document, "digital identity" has the meaning set out in the Glossary at Attachment A

- establishment of an independent statutory officeholder to oversee the System and accreditation scheme – the Australian Government Digital Identity Oversight Authority
- appointment of advisory boards to advise the Oversight Authority
- applications for accreditation and onboarding and related matters
- notice of decisions
- internal and AAT review of decisions
- registers to show entities that are participating in the System or are accredited only
- privacy and other consumer safeguards, security and fraud-prevention requirements applying to participants in a digital identity system
- compliance powers, with show-cause letters prior to the taking of compliance action
- for participants in the System:
  - obligations, including requirements for onboarded accredited entities that are service providers to enter into agreements with the Oversight Authority
  - a charging framework
  - a liability and redress framework
  - enforcement including triggering of some parts of the Regulatory Powers (Standard Provisions) Act 2014 ('Regulatory Powers Act'), namely the civil penalty provisions, enforceable undertakings and injunctions
- obligations for accredited entities (i.e. entities not using the System)
- a trust mark framework with a civil penalty for unauthorised use by a person.

The primary legislation itself is not proposed to be prescriptive, but establish powers to regulate in several areas, with further specific details to be set through subordinate legislation. Some aspects of the expected regulatory costs will be determined by the specifics of this subordinate legislation.

Further detail on the regulatory measures contained within the Exposure Draft package and their impact on regulated entities, is set out in Section 9 Likely net benefit of Option 3 – Dedicated regulatory scheme.

Charging framework

As outlined above, proposed legislation under this Option 3 would enable the introduction of a System charging framework. Whilst the details of this framework remain under development and the subject of ongoing consultation, it is expected to follow the broad principles below.

The charging framework may provide for:

- fees for the assessments necessary to consider an application for accreditation, reaccreditation and annual accreditations
- charges for use of the System by participants.

The framework will not directly impose charges on individuals using the System, but will not regulate fees charged by relying parties wanting to access the System to provide a service to an individual. The Bill will allow the Australian Government to charge and set out criteria for government charging, and secondary legislation (likely rules) will provide the amount of the charge, and /or any formula for determining the charge, as well as charging arrangements. The charging framework will be developed in compliance with Australian Government charging framework and related requirements and guidelines.

Development of the System charging framework has continued throughout 2021, through consultation with key stakeholders including state and territory governments, the private sector and a range of Australian Government departments and entities. This and other ongoing Program consultation is described in more detail at Section 10 Consultation to date and future roadmap.

Mitigating regulatory impact

A key feature of Option 3, reflected in the Exposure Draft package, is a focus on mitigating complexity and regulatory burden for Australian businesses, individuals and government. To that end, it seeks to leverage existing laws, definitions and concepts wherever possible instead of creating a unique set of arrangements.

Key examples of this include:

- existing definitions and terminology from the Privacy Act used within the Exposure Draft package (such as personal information). This enhances consistency and also mitigates regulatory impact, as many entities should have an existing level of familiarity with these concepts and the regulatory framework will leverage known processes and mechanisms
- continued use of System-specific terminology and concepts that are already established within sources such as the TDIF and National Identity Proofing Guidelines. This will be of particular benefit for entities which are already participating or interacting with the System prior to the legislation being passed
- the intent to adopt terms and processes from other legislation (and pending legislation) as relevant, for example, 'cyber security incident' from the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* and the 'adverse assessment and recommendations' process from the *Data Availability and Transparency Bill 2020.*

6 Approach to determining likely net benefit of options

6.1 Overview

The following sections outline the impacts (both positive and negative) of each option on relevant stakeholder groups, in order to determine the likely net benefit of each option. This impact assessment is conducted at two levels:

- Overall impacts – including economic, competition, social, environmental or other
- Regulatory impacts – a subset of the overall impacts, specifically focused upon the regulatory impacts involved in each option and the burden on regulated entities.

Each level of analysis takes a different approach, and focuses on different stakeholder groups, as set out in further detail below.

6.2 Overall impacts

This RIS considers the overall impacts (both costs and benefits) of each option across the broad stakeholder groups that are likely to be affected – individuals, businesses, government and the community. These impacts may be economic, competition, social, environment or other. For the purposes of this assessment, the stakeholder groups have been defined as follows:

- **Individuals** – refers to private individuals, specifically those who choose to participate in the System, by selecting an identity provider and using their Digital Identity to transact with available services online. Individuals who are potential System users are also considered
- **Businesses** – refers to private sector entities who may wish to be accredited or participate in the System. The impacts of each policy option will differ depending on businesses' intended form of participation, as well as business size/type/sector

- **Government** – includes the Australian Government, as well as state, territory and local governments. The impact analysis specifies the levels of government to which a particular cost or benefit applies, as the impacts of each policy option may vary. This reflects the fact that the Government's current involvement in the System exceeds that of state, territory and local governments. Where the context specifies, this category also includes Government Business Enterprises (GBEs)
- **Community** – involves consideration of impacts on both the community as a whole – being a collective of individuals – and community sector organisations.

These overall impacts, including the likely distribution of costs and benefits, are discussed primarily qualitatively. Where data is available permitting quantification of these broader impacts, this has been done.

6.3 Regulatory impacts

Regulatory costs form a subset of the overall impacts (costs and benefits) of the System. It is an Australian Government requirement that any proposed new or changed regulation must include quantification of the increase or decrease in regulatory costs imposed on businesses, community organisations and individuals. The identification and quantification of regulatory costs must be conducted in accordance with the Regulatory Burden Measurement Framework.

In accordance with government requirements, the final version of this RIS will calculate the estimated regulatory burden for all options. The approach taken to date, and future actions to measure the regulatory burden, is set out below.

6.3.1 Regulatory costs

Under the Regulatory Burden Measurement Framework, only certain costs associated with the System are categorised as 'regulatory'. The primary categories of regulatory costs are:

- **Administrative compliance costs** - costs incurred by regulated entities primarily to demonstrate compliance with the regulation. For example, the time

and costs associated with keeping records, making an application and notifying government of certain activities

- **Substantive compliance costs** – costs incurred to deliver the regulated outcomes being sought. Examples: costs of training employees on regulatory requirements, professional services required to meet regulatory requirements
- **Delay costs** – the expenses and loss of income incurred by a regulated income as a result of an application delay, or an approval delay.

There are several types of costs specifically excluded from the Regulatory Burden Measurement Framework. These include, for example, opportunity costs, business-as-usual costs, enforcement /compliance costs (such as fines for failing to comply with regulation), and government-to-government regulation. Importantly, fees for services (such as any charges payable under a future charging framework) are not categorised as regulatory costs, and therefore will not be quantified under this RIS.

6.3.2 Regulated entities

The overall impacts consider flow-on impacts of the regulation on a broad range of stakeholders across the Australian community. However as the regulatory impact assessment focuses only on regulatory costs, by definition it considers regulated entities only. Stakeholders to which regulation of the System would apply, and therefore the focus of this regulatory cost analysis, are:

- **Onboarded accredited entities –** Entities that are accredited and onboarded to the System as either APs, CSPs, IDXs and/or IDPs
- **Accredited entities –** Entities accredited for a particular role (as above), which have not been onboarded to the System
- **Relying parties** – Rely upon verified information provided through the System to provide a digital service. Must be onboarded, but not accredited.

The regulatory costs and impacts have been considered through the lens of these specific stakeholder groups. Although governments of all levels can participate in the System in the above roles, government-to-government regulation is excluded from the Framework. (This exclusion does not, however, apply to GBEs and public universities. Noting the important role that GBEs such as Australia Post may play in

the System in the future (with Australia Post's identity solution already accredited within the System), these types of entities are included in the regulatory burden measurement.)

6.4 Impact analysis conducted to date

This RIS focuses on identifying broad *categories* of anticipated costs and benefits arising from the proposed policy options. A comprehensive scan has been conducted of available literature and evidence on the impacts of the System – both its potential benefits for individuals, businesses, government, community, and the economy, and potential regulatory costs of the policy positions.

There are a range of digital identity programs in operation or under development around the world, including in Canada, New Zealand, Sweden, India, the United Kingdom and Estonia. The impacts of digital identity programs in these different country contexts have been examined, with analysis then considering their applicability to the Australian context. In some instances, this process identified costs or benefits which are unlikely to be realised through the Australian Government Digital Identity System, which were then excluded from analysis. For example, in India one of the most significant benefits of digital identity's expansion has been a major reduction in corruption, due to the reduced influence of local government officials in verifying and endorsing identity. This was not assessed as relevant in the Australian context because of significantly lower levels of government corruption risk.

Consultation conducted by the Program also supported the identification of potential costs and benefits arising from this proposed regulation. Submissions to recent public consultation processes were particularly examined to identify any areas which had not already been identified internally. Consultation with Program subject matter experts also supported identification of areas where the costs and benefits of Australia's proposed approach may diverge from those observed internationally. This highlighted the differential impacts expected for onboarded accredited entities compared with relying parties (as detailed in Section 9 Likely net benefit of Option 3 – Dedicated regulatory scheme).

6.5 Future analysis

The purpose of public consultation on the following sections is to:

1. validate the expected overall impacts
2. better understand /quantify the potential regulatory costs.

In the next and final version of this RIS, the overall impacts will be updated to include any additional economic, social or other costs identified through the consultation process. Additionally, the information provided on the regulatory burden of proposed options will permit validation of the quantified costs and their whole-of-society impact – also to be included in the final RIS.

The following three sections describe the costs, benefits and overall likely net benefit for each option, in accordance with the methodology described above.

7 Likely net benefit of Option 1 (status quo)

Option 1 involves continued existence of the System as it currently operates, with no regulatory action. As such, there are no changes to the costs and benefits currently experienced by each stakeholder group. For completeness, these costs and benefits are described below.

7.1 Overall impacts

7.1.1 Individuals

Under the status quo arrangement, individuals can access the System through myGovID (the Australian Government's digital identity provider), and transactions within it continue to be limited to Commonwealth services and entities. In their interactions with participating Australian Government services, individuals benefit from improved speed and convenience across a range of transactions – with over 75 Government agencies currently involved in the System. However, the exclusion of non-Australian Government agencies as relying parties (except in limited circumstances) and charging onboarded accredited entities under the status quo constrains the range of places and contexts in which individuals can use the System.

The implications of the status quo arrangement for individuals are two-fold. Firstly, whilst individuals have protections under the TDIF in areas such as privacy, collection and use of data, and storage of biometric information, this only applies in relation to accredited services available in the current System (primarily Australian Government). Secondly, the full efficiency benefits of the System for individuals cannot be realised due to the System's ongoing inability to expand to the private sector. Legislation is required to bring non-Australian Government relying parties and charging onboarded accredited entities within the System, allowing full access to both government and private sector verification.

Under the status quo, where private sector entities are not able to participate in the System as relying parties nor as onboarded accredited entities with a legislative ability to charge, future growth in the number of participants entering the System as onboarded accredited entities (for example, as IDPs or APs), may also be inhibited. While the System currently facilitates transactions with a number of Australian

Government agencies, the ongoing benefits of scale and potential market uptake would be greatly reduced if the pool of relying party participants remains restricted to such entities. Individuals will continue to face limitations in their choice of identity provider, being the existing myGovID and System services.

Individuals who use the System incur no direct costs, as their use within the System of the two identity products listed above remains free. There is no regulatory burden on this stakeholder group. If the status quo were maintained, individuals would retain access to the current benefits of using the System with available Government services. However, they would forego the additional or compounded benefits that would arise from the System's expansion to non-Australian Government relying parties and charging onboarded accredited entities.

These foregone benefits are discussed in greater detail under Option 3, but include:

- improved speed and convenience in interactions with a wider range of entities – particularly as individuals typically interacts on a regular basis with private sector providers, such as banks, utilities and telecommunications providers
- reduced risk of identity fraud and associated financial loss – as financial services providers and other entities, which are the most common sites for this type of fraud, cannot participate in the System as relying parties
- increased choice and control in how they engage with the System – as they will likely be limited to using government and quasi-government identity solutions
- strengthened consumer protections enabled both by the conversion of voluntary TDIF requirements into law and their expansion to all System participants – as these will not apply.

Assessment of net expected benefits: Under the status quo, individuals continue to benefit from the significant efficiency gains arising in interactions with Australian Government services currently participating in Digital Identity. This leads to an overall net positive benefit for individuals, compared to a situation where the System is not available. However, considered in relative terms the net benefits of the status quo for current and potential individual users of the system are lesser than those available under other options that may enable System expansion.

7.1.2 Businesses

Under the status quo, small, medium and large enterprises face no regulatory costs because their participation in the System is generally not supported. As with individuals, this results in considerable foregone benefits for this major segment of Australia's economy. These foregone benefits differ according to the potential role that businesses would seek to play in the System – either as onboarded accredited entities or relying parties.

Onboarded accredited entities

Whilst there are no legal impediments to businesses becoming onboarded accredited entities under the status quo arrangements, there is no legislative basis for charging for services within the System under the status quo. This practicality is likely to deter most potential onboarded accredited entities, particularly small to medium enterprises.

Similarly, potential large enterprise onboarded accredited entities would have no legislated ability to charge for their services. This would result in foregone benefits in relation to new business opportunities, and those expected to accrue through innovation and expansion of existing identity products or solutions.

Under the status quo, all potential onboarded accredited entity businesses would forego the legal protections associated with a dedicated regulatory scheme. Specifically, the proposed legislation includes a liability regime, enabling the Australian Government to indemnify onboarded accredited entities from civil proceedings and liability if they have provided the service in good faith and in compliance with the regulatory scheme (whilst requiring them to assist users where there has been an inappropriate disclosure of information, identity theft, or cyber security incident). The benefits of this indemnity would significantly reduce onboarded accredited entity businesses' exposure to financial loss and the risk of civil litigation.

Relying parties

The status quo does not allow private sector entities to participate in the System as relying parties. The legal rationale for this is outlined in Section 3.2.1 No legal basis for participation of non-Australian Government agencies as relying parties, nor for a

charging framework. As a result, small, medium and large enterprises, who would otherwise seek to participate in the System, forego all benefits expected to accrue under a dedicated regulatory scheme. These include:

- efficiency and productivity improvements associated with reduced manual handling of customer identification documents, reduced staff resourcing requirements associated with identity verification and increased speed of verification with other participating entities. These foregone benefits are potentially significant for many small and medium enterprises, who are heavily reliant on manual handling and staff resourcing to conduct business activities
- new business opportunities available because of easy and cost-efficient access to verified attributes
- reduced instances of financial loss associated with customer fraud, as well as efficiencies gained through reduced investigation and prosecution of fraud events.

These foregone benefits are expected to represent the most significant share of indirect costs associated with maintaining the status quo.

Assessment of net expected benefits: Under the status quo, there are ongoing positive direct and indirect benefits for business users of the System in terms of the efficiency and productivity gains. However, under this option, a significant share of businesses are unable to participate in the System as relying parties or onboarded accredited entities. Those which may, in theory, participate lack the incentives to do so. If the status quo is maintained, the indirect costs for businesses are likely to be significant when comparing the status quo arrangement with the benefits available under a dedicated regulatory regime. This means that on a relative comparison, the net expected benefits for business of the status quo are likely to be lesser than under other options.

7.1.3 Government

While a continuation of the regulatory status quo arrangement may offer some certainty for government stakeholders, the System's potential benefits may not be fully realised. In particular, the status quo may jeopardise the Australian Government's commitment to 'choice' as a fundamental principle of the System.

Access to a pool of Australian Government-only services and a low number of Identity Providers means Australians' ability to choose where and how they engage with the System is inherently limited.

Currently, Australian Government entities participating in the System benefit from increased efficiency of customer operations and productivity gains, arising from reduced manual handling. These benefits will endure for Government agencies if the status quo arrangement were maintained.

However, under the status quo, these benefits do not extend to state, territory or local governments. As such, with the exception of current Government participants, other levels of government forego similar benefits to private sector businesses, including:

- improved efficiency of customer operations
- reduced manual handling, resulting in time and cost savings
- reduced time and effort undertaking "de-duplication" - reducing the instances of duplicated entries within alternative identity systems (as this de-duplication would be automatically done by the identity exchange under an expanded System)
- reduced instances of identity fraud resulting in the payment of benefits or supply of services to which people are not entitled.

As government services increasingly move online, there is a growing need for digital options to verify identity. A lack of such options undermines the service experience and efficiency gains associated with digital delivery of Government services. In the event that state, territory and local governments are unable to participate in the System, it is likely that alternative solutions will need to be developed by individual jurisdictions – at significant time and cost impost. Therefore, the status quo imposes potential indirect costs on these levels of government, by requiring them to establish and invest in alternative identity verification solutions.

Assessment of net expected benefits: The benefits currently conferred on Australian Government agencies participating in the System are expected to offset the foregone benefits and indirect costs associated with the status quo option for state, territory and local governments. However, the larger number of sub-national

government entities and higher combined volume of transactions means the foregone benefits of an option that does not allow system expansion are still considered significant.

7.1.4 Community

Under the status quo, community stakeholders derive limited benefits from the System, as they are largely excluded from participation. As with businesses and government entities who may participate as relying parties, community sector organisations face foregone benefits, including:

- improved efficiency of customer operations and reduced manual handling
- reduced instances of identity fraud resulting in the supply of services or goods to which people are not entitled.

As entities engaged in charitable or not-for-profit activities, community organisations may in fact benefit more significantly from the above efficiencies than their counterparts in the for-profit sector, and conversely are more adversely impacted by foregoing these benefits.

The benefits accruing to the broader Australian community largely relate to trust and confidence in the System. If Australians collectively trust the System and have confidence that it will support their privacy, autonomy and control, they are more likely to participate as users, leading to collective economy-wide benefits. Under the status quo, the protections and provisions of the TDIF are not legislatively enforceable, nor are they overseen by a permanent governance authority with legislative functions and powers. This arrangement is less likely to support strong community trust and confidence in the System's integrity and safeguards, than (by comparison) the dedicated regulatory scheme option. Option 3 also offers enhanced protections beyond those currently included in the TDIF and existing privacy legislation (for example, in relation to biometrics and commercialisation of data). These are entirely foregone under the status quo.

Assessment of net expected benefits: Compared to an expanded System underpinned by regulation, community organisations and the community as a whole incur substantial foregone benefits (such as efficiencies for community organisations seeking to become relying parties, as well as strengthened trust and confidence).

7.2 Regulatory impacts

As the status quo envisages that the System continues operating with no dedicated legislative or regulatory framework, there are no changes to current regulatory impacts. Even if there were, the ongoing restrictions on non-Australian Government involvement in the System under this option means that they would not be imposed upon the private sector (business, community or individuals). In the following sections, this current state is treated as the "baseline" against which the potential regulatory impact of Options 2 and 3 are expressed.

7.3 Likely net benefit

As described in Section 2.4 Benefits and value of the System, the status quo arrangement continues to confer notable benefits on current Australian Government agency participants, some businesses, and Australians– insofar as access to the System and the broader Australian Government framework would be ongoing, in its current form. However, these benefits accrue only to a subset of those entities and businesses capable of participating in the System through other options canvassed in this RIS. Under the status quo, there are no additional or changed regulatory costs incurred by any stakeholders.

Despite the many proven benefits of the System, and the absence of regulatory costs, under Option 1 individuals, businesses, governments and the community will incur substantial foregone benefits relative to other options. The full potential of the System can only be realised through its expansion to a far wider range of entities and service contexts – an expansion which cannot be achieved through the status quo arrangements.

Consultation question(s)

(1) Are the impacts of Option 1 accurately described as related to your entity? Are there any other impacts (negative, positive or neutral) of the System continuing without regulation, that are not mentioned above?

8 Likely net benefit of Option 2 (leverage existing regulatory frameworks)

As with Option 1, Option 2 supports System involvement from Australian Government agency participants only and Australian individuals. However, this option will not support an expansion of the System to non-Commonwealth relying parties, nor provide a legislative charging framework for use by non-Australian Government onboarded accredited entities. With this in mind, Option 2's impacts on each stakeholder group are addressed below.

8.1 Overall impacts

8.1.1 Individuals

Under Option 2, individuals would continue to enjoy the efficiency and productivity benefits gained from interactions with current Australian Government agency participants in the System. Further, individuals will benefit from the strengthening of some privacy and consumer safeguards, which currently apply in a non-legally enforceable manner to participants within the TDIF. This option would make existing protections legally enforceable, likely with reviews, monitoring and reporting conducted by a nominated APP Code Administrator. (The OAIC's guidelines for developing codes, issued under Part IIIB of the Privacy Act, outline a range of recommended powers and functions of the Code administrator.) However, Option 2 would not deliver new or additional consumer protections for individuals using Digital Identity. While any new protections would remain subordinate to primary legislation, this benefit represents a strengthened position on privacy and security, compared with the status quo's non-legislative model of compliance with the TDIF.

As private individuals can continue to use the System's services, accompanied by legislative privacy protections, enhanced trust and confidence as a result of this option may increase uptake of the System by individuals. However, Option 2 is not expected to substantially increase the range of agencies or entities participating in the System because it does not address the barriers to participation by private sector entities or state, territory and local governments. As a result, individuals are expected to forego the compounded efficiency and productivity benefits, reduced risk

of identity fraud and increased choice, which would be available under a dedicated regulatory arrangement.

Assessment of net expected benefits: Under this option, individuals are expected to experience increased benefits through stronger enforceability of existing consumer protections, when compared with the status quo arrangement. However, because this option does not enable the expansion of the System to more participants beyond the status quo, individuals will continue to forego the additional benefits available under a dedicated regulatory scheme. These costs are expected to outweigh the benefits available under Option 2, meaning the net expected benefit for individuals, compared with Option 3, is likely significantly lesser.

8.1.2 Businesses

Option 2 would not alter any of the existing legal barriers preventing participation by businesses in the System. Businesses would continue to be eligible to participate in the scheme as onboarded accredited entities (for example, by becoming an Identity Provider), but are unlikely to do so given the legal inability to charge for these services. Nor would businesses be able to do so as relying parties (for example by using myGovID to verify customer identities). This leads to slightly different benefits and costs for these two categories of potential participants, as outlined below.

Onboarded accredited entities

Under Option 2, onboarded accredited entities would be expected to face increased regulatory costs compared with Option 1, but lower regulatory costs than under Option 3. This is because the provisions of the TDIF would take on the status of an enforceable Code, rather than being written into primary law.

While onboarded accredited entities may incur reduced compliance costs under Option 2 than would be the case under Option 3, they would also see reduced benefits. This is primarily because the Code would not encompass the proposed indemnity arrangements against loss arising from the provision of a fraudulent identity. As identified under Option 1, this is a significant potential benefit for businesses which would be foregone under all options except the legislative approach.

As with Option 1, businesses would notionally be able to join the System as identity providers and therefore expand their service offerings or market presence. In practice, however, the incentive to do so would continue to be limited (particularly for small and many medium sized businesses) because this option does not enable them to charge for services provided within the System.

Relying parties

Option 2 does not address the existing restrictions on businesses participating in the System as relying parties. Businesses which are potential participants would therefore not experience regulatory costs due to being excluded from participation in the System. These businesses would also incur the same foregone benefits outlined under Option 1, which have been noted to be the largest potential source of economic and productivity gains.

Assessment of net expected benefits: The System's major potential benefits for business arise from its expansion to a broader range of entities beyond government entities. This would both increase the productivity and efficiency gains for relying party businesses and incentivise the entry into the System of more onboarded accredited entities, who can then pursue new market opportunities. Option 2 does not address the existing barriers to participation by business in either of these capacities, meaning foregone benefits would remain. As a result, the net expected benefit is likely to be comparatively lesser for businesses than under Option 3.

8.1.3 Government

Option 2 does not affect the range of government entities which can participate in the Australian Government Digital Identity System. It is expected that uptake by Australian Government entities would continue to increase, with a Code providing somewhat improved clarity and transparency in relation to the obligations of participating entities. The benefits accruing to participating Government entities under the status quo arrangements would also continue to apply, including increased efficiency (through reduced manual processes and the reduced need for de-duplication), productivity and reduced instances of identity theft or fraud. However, existing restrictions on the participation of state, territory and local governments would remain, limiting the opportunity for these benefits to flow to entities outside the Australian Government.

In line with the above discussion of business impacts, government entities which are already fully complying with the TDIF would not be expected to incur additional costs as a result of leveraging existing regulatory frameworks. This should be the majority of Australian Government participants currently operating within the System. However, given that a Code would impose additional obligations over and above those within the Privacy Act, some new entities or Departments may need to upgrade their practices, infrastructure or procedures to comply with the Code ahead of joining the System.

Compared with Option 3, this option is expected to result in less costs to the Australian Government in relation to implementation and ongoing oversight of the System. The approach may introduce added complexity for the System's implementation and operation on an ongoing basis. The source of the System's legislative authority would reside in legislation administered by a separate department and portfolio. While this may introduce some added complexity and potential administrative and governance burdens, Option 2 does not involve the establishment of a permanent Oversight Authority. This means costs savings arise from associated investments in governance, assurance, compliance and enforcement that would be required to support the dedicated regulatory scheme option. The specific extent of these cost savings would depend on decisions of Government about the reasonable resourcing required to give effect to Option 3. While these potential savings may be considered a benefit in the specific context of the Australian Government's budget, they would come at the expense of significant foregone benefits for state, territory and local governments, businesses and individuals, as outlined in this section.

Assessment of net expected benefits: The benefits accruing to the Australian Government under Option 2 are notable, but broadly equivalent to those available under the status quo, with the addition of some regulatory cost savings. However, the foregone benefits for state, territory and local governments incurred from their exclusion from the System are also expected to remain significant. Taking these different impacts across levels of government into account, and the potential benefits available under a dedicated regulatory scheme, the net expected benefit of Option 2 is likely to be lesser than that available under Option 3.

8.1.4 Community

Option 2 does not address the existing restrictions on community organisations' participation in the System as relying parties or as onboarded accredited entities with a legislative ability to charge. As such, community organisations who would otherwise wish to participate in the System would experience no added costs under Option 2. However, these organisations also forego the same benefits as outlined under Option 1, including substantial productivity and efficiency gains which would be particularly valuable to the community sector.

Leveraging existing regulatory frameworks may serve to increase the Australian community at large's understanding of the System, and their trust and confidence in its protections. However, the consequential impacts on increased uptake would remain inherently limited, with the exclusion of some government and all private sector entities.

Assessment of net expected benefits: The Australian community's levels of trust and confidence in the System may be slightly improved by Option 2, as a result of increased privacy and security protections. However, trust and confidence in the System would be substantially better supported under Option 3. For community organisations, the costs of Option 2 are likely to outweigh the benefits, as such organisations' participation as relying parties is not supported by Option 2.

8.2 Regulatory impacts

Option 2 involves leveraging existing regulatory systems to provide protections in key areas such as privacy. However, this Option does not address the existing legal restrictions on involvement in the System of non-Australian Government relying parties, and would not establish a legislative basis for onboarded accredited entities to be able to charge. As a result, private sector or community organisations would not be considered 'regulated entities' under this Option. The primary participants in the system (both relying parties and onboarded accredited entities), would continue to be Australian Government agencies, which are not within the scope of the Regulatory Burden Measurement Framework.

One exception to the above, is GBEs such as Australia Post, which are considered within the scope of the Framework. Under this Option 2, GBEs would be required to comply with the provisions of a Code registered under the Privacy Act. As set out in Section 3.2.2 Lack of trust in System's privacy and security safeguards, the primary shortcoming that this Option 2 would be seeking to address, is the inconsistency in privacy obligations across APP and non-APP entities. The code envisaged in Option 2 would apply universal, consistent obligations across all entities using the System, up to a minimum standard consistent with Australian Government privacy legislation.

As GBEs are already bound by the Privacy Act, including the NDB Scheme, the additional regulatory cost of complying with any Privacy Code under this Option 2 is expected to be negligible. As participation in the System is voluntary for GBEs and other participants, it would be expected that GBEs only use the System if these eligible regulatory costs were offset by the broader economic and commercial benefits available.

Based upon initial calculations, as outlined in Appendix E Regulatory costs: methodology and assumptions, the annual regulatory cost range of Option 2 for GBEs has been estimated at $1,461–$2,630 (for relying parties) and $2,082–$3,543 (for participants in the System). This is the estimated amount it would cost an entity to comply with the proposed regulations, based on the time and labour cost of undertaking required activities (i.e. it is not a 'fee' or 'charge' to use the System). Section 6.3 and Appendix E provide further detail regarding the methodology by which these estimates have been developed, which is consistent with the Australian Government's Regulatory Burden Measurement Framework. Importantly, this regulatory cost figure does not constitute nor indicate a proposed charge for using the System.

8.3 Likely net benefit

The above analysis indicates that Option 2 may offer some efficiency and productivity benefits for select stakeholder groups who already have legislative authority to use and be part of the System – notably, individuals and governments. Further, individuals and the Australian community may benefit from slightly enhanced privacy and security mechanisms. However, all stakeholders are expected to experience significant foregone benefits which would be realised if the System

were expanded to include non-Australian Government relying parties, under a dedicated regulatory arrangement.

Consultation question(s)

(2) Are the impacts of Option 2 accurately described as related to your entity? Are there any other impacts (negative, positive or neutral) not mentioned above?

9 Likely net benefit of Option 3 (dedicated regulatory scheme)

As described in Section 5.3 Option 3: Dedicated legislation to establish new regulatory scheme, the detail of proposed legislative and regulatory provisions involved in this Option 3 is currently being validated through public consultation on the Exposure Draft package. This section presents a discussion of the likely impacts of the measures currently under consideration, and will be updated to account for any changes arising from the consultation process.

9.1 Overall impacts

9.1.1 Individuals

The benefits to individuals of Option 3 can be articulated at two levels, those arising:

a. indirectly from the expansion of the System enabled by the legislation

b. directly from the protections and safeguards offered by the regulatory scheme itself.

(a) Expected benefits of expansion

This legislation will provide the foundations for a much wider range of private sector and state, territory and local government entities to use the System to verify their customers. For individuals, this means being able to interact and transact with greater speed and efficiency with a wider range of organisations and businesses. Internationally, digital identity has been taken up by providers in a number of sectors that Australians interact with regularly, particularly:

- banks and financial institutions
- utilities and telecommunications providers
- social care service providers (for example, healthcare and childcare)
- state and local government authorities.

Interest in TDIF accreditation has also been received from international IDPs who want to offer digital identity services in Australia. Enabling the participation of such

an expanded range of organisations and businesses within Australia is an expressed policy objective of this regulatory action, as discussed above in Section 4.3 Objectives for government intervention.

By removing the need to present physical identity documents and set up multiple identity profiles across these diverse service providers, the time required for individuals to verify their identity with service providers can be reduced from hours to minutes. Economic modelling indicates increased uptake of the System just in relation to university and vocational education services alone could result in time savings for individuals, worth between $12.7 million and $38.7 million a year (source: *Economic Benefits of Digital Identity* 2020, KPMG). These time savings grow as the range of places individuals can use the System expands.

The expansion of the System to private sector participants is also expected to confer benefits for individuals in relation to the avoided costs of identity loss, theft and fraud. Across 2018–19, ACCC's Scamwatch received 55,909 reports of "attempts to gain personal information", with financial losses associated with these reports having increased by 65% from the previous period (from $8 million to $13 million). The System reduces the risk of identity fraud both because it provides for a higher standard of secure verification, and because it reduces the likelihood of physical identity documents being lost or stolen.

With a significant amount of identity fraud occurring in relation to transactions with banks and other financial services providers, the System's expansion to these providers presents a meaningful opportunity to reduce the individual costs of this kind of crime. The COVID-19 pandemic has led to increasing numbers of online transactions and as a consequence, increasing reports of identity fraud. The ACCC reported an 84% surge in identity theft scams and 75% surge in phishing scams during 2020. As with the time savings benefits, the avoided costs of identity fraud would be expected to grow as the number of private sector providers adopting the System increases. The costs of identity fraud to an individual can be both financial, (through lost funds) and personal (through, for example, the time taken to rectify/mitigate the fraud and reputational or other personal damage inflicted).

(b) Expected benefits of regulatory scheme

The legislation's mandate that the System remain voluntary for individuals offers a considerable benefit, particularly for individuals who, for various reasons, may prefer not to engage with government-provided identity products. Legislation will also ensure that relying parties may not compel individuals to use the System in order to access services and, with some exceptions, must continue to provide alternative options for identity verification (e.g. telephone, in-person and paper-based options). This means user choice will be strong and formally embedded within the System through the legislation.

The regulatory scheme will enhance privacy protections for individuals. The proposed protections would represent a strengthening of those currently applying to the System by virtue of existing privacy legislation, including the Privacy Act, because they would:

- restrict the creation and use of single identifier
- impose strong conditions upon the use of biometric information
- impose data breach action and reporting requirements which are currently not in place
- restrict the capacity for aggregation and on-use of personal data.

Additionally, the legislation would establish a permanent Oversight Authority with the ability to make and enforce rules on the System's security and integrity, further strengthening protections for individuals compared with current arrangements that lack legal enforceability. As a result, individuals will benefit from strengthened, legally entrenched privacy protections, and improved avenues for recourse, in the event of the misuse of personal information, data breaches or identity fraud.

The requirement that positive consent be sought from individuals on each occasion prior to the provision of a service, will ensure individuals enjoy strong levels of autonomy and control in how and when they interact with the System. This is in contrast with other de facto identity solutions made available by private companies, which are increasingly being used to transact with companies and services online.

(c) Expected costs of regulatory scheme

The policy intent underpinning the proposed regulatory scheme is that individuals will not be directly charged for using Digital Identity, however it will not regulate fees charged by relying parties accessing the system to provide a service to an individual. This means individuals interacting with the System may be charged to do so by a relying party. Given the voluntary nature of the System, and the requirement that alternatives to using the System remain available, relying parties would need to ensure that such charges are set at a level which incentivises individuals to use the System, rather than the alternatives available. In relation to regulatory costs, the specific provisions of the regulatory scheme would apply primarily to onboarded accredited entities and – in some instances – relying parties. As a result, there are not expected to be any regulatory costs to individuals arising from this option.

There is a small risk that the expansion-related benefits outlined above become foregone benefits for individuals if the regulatory burden was so great as to prevent private sector providers participating in Digital Identity. However, this does not appear to be a significant risk in light of the balance of costs and benefits for these participants, discussed below.

Assessment of net expected benefits: In light of the significant expected benefits for individuals – direct and indirect – enabled by this dedicated regulatory scheme, and the minimal individual costs associated with it, the balance of net benefits is expected to be strongly positive for individual Australians.

9.1.2 Businesses

Option 3 provides the legal authority for businesses to engage with, and participate in, the System in a number of different contexts. Under the status quo, businesses can already become an onboarded accredited entity (but are unlikely to be active within the System due to the absence of a charging framework), in order to play a role as one or more of the following:

- IDP – for example, a consortium of banks may choose to develop a private sector identity verification product offering parallel services to myGovID
- AP – for example, universities may choose to participate in the System to provide verification services relating to qualifications.

Businesses participating in the System as onboarded accredited entities are expected to be larger corporations and entities. This is because of the infrastructure and investment costs associated with delivering identity and attribute services.

However, under Option 3, businesses could also engage with the System as relying parties. For example, utilities providers may connect with one or more IDPs to undertake identity verification on new customer accounts. Businesses participating in the System as relying parties are expected to span a diversity of sizes, potentially including small businesses and sole traders which are currently exempt from the Privacy Act and other data handling and security regimes. As noted throughout this assessment, the provisions of the proposed regulatory scheme primarily apply to onboarded accredited entities. For this reason, the expected benefits and costs for business have been assessed separately depending on whether they are onboarded accredited entities or relying parties.

Onboarded accredited entities

(a) Expected benefits of regulatory scheme

Currently, private sector entities wishing to participate in the System as onboarded accredited entities are not supported by a robust system of regulatory safeguards and frameworks. For businesses considering making investments necessary to participate in the System, the regulatory scheme (and the governance structure it establishes) provides a clear basis upon which to assess the expected long-term benefits, risks and costs of doing so.

Under Option 3, legislation would also establish the framework and principles for a charging regime associated with use of the System. The details of this regime will be determined in secondary legislation but are expected to facilitate charging by onboarded accredited entities for the use of their services (e.g. identity service products or attribute verification). The establishment of the charging regime provides a basis for onboarded accredited entities to generate significant commercial benefits through the aggregation of fees received as a service provider within the System. The exact quantum of these benefits will be determined by the regulatory scheme's charging framework.

The regulatory scheme will strengthen safeguards for non-Australian Government agencies participating in the System. Specifically, proposed liability provisions will

enable the Commonwealth to indemnify onboarded accredited entities from any loss that results from, for example, the provision of a fraudulent identity, provided the entity has acted in good faith and demonstrated compliance with all System rules and regulations. This would significantly mitigate the risks of service provision within the System, compared with the status quo in which such protections are not available to non-Australian Government agencies.

Further, private entities who currently provide digital identity services as part of their commercial offering, such as credit and background checking agencies will benefit from the possible evolution of their service offering to the System – supported by the new regulatory scheme. This demonstrates Option 3's capability to not only facilitate the creation of new digital identity products, but to create opportunities for innovation in existing private sector forms of identity verification.

(b) Expected costs of regulatory scheme

The legislation will require potential onboarded accredited entity businesses to comply with the requirements of the Privacy Act (as applicable to their System-related activities). Where businesses do not already operate in alignment with the Privacy Act's requirements, the costs of compliance are potentially significant.

The Privacy Act mandates a range of measures for data collection, storage and destruction, among others, which are unlikely to be standard practice for smaller businesses or private firms. This potential cost is mitigated by the fact that entities engaging with the System as onboarded accredited entities are anticipated to be larger private sector businesses. As previously noted within this RIS, all businesses with annual revenue above $3 million are already subject to the provisions of the Privacy Act. These businesses would therefore not incur additional compliance costs related to this requirement, where they are already subject to the Act's provisions.

Businesses wishing to become onboarded accredited entities are also likely to incur costs associated with other non-privacy related requirements mandated by the regulatory scheme. These are expected to include:

- administrative costs associated with reporting requirements to the future Oversight Authority
- System and infrastructure security requirements established to meet the standards of accreditation

- compliance monitoring to ensure System use and access is provided in line with authorised uses
- oversight, restrictions and associated requirements of managing biometric identifiers, and the creation and use of single identifiers
- monitoring and compliance for data breach notification processes
- compliance with any other rules imposed by the Oversight Authority, to address security of the System.

It should be noted that some of these costs would be incurred in the development of any private sector digital identity product or solution, regardless of whether it is regulated by the government. It should also be noted that joining the System as an onboarded accredited entity is entirely voluntary. This means that businesses which assess the costs of compliance as outweighing the specific benefits for their organisation, are fully able to choose not to participate.

Businesses may also incur opportunity costs associated with losing access to, or ownership over, customer data. For private sector businesses, the aggregation and sale of customer data may present a meaningful commercial opportunity. The proposed regulatory scheme may affect an organisation's practical or legal ability to capitalise on such opportunities. This is because providers may no longer collect or hold themselves some information about individuals, and the regulatory scheme contains specific restrictions on the on-selling or use of customer data collected through the System. The extent of this potential opportunity cost would vary significantly depending on the extent to which companies who seek to become onboarded accredited entities currently engage in commercial activity associated with data aggregation and on-selling, and therefore cannot be reliably estimated.

Relying parties

(a) Expected benefits of regulatory scheme

Legislation under Option 3 will enable private sector entities to participate in the Program as relying parties for the first time. This will improve speed of interaction across a wider range of government and private sector entities, where multiple entities or businesses are involved in conducting a transaction. The resulting time and cost savings will generate significant productivity gains for organisations which frequently need to verify the identity of their customers. Relying parties will also

benefit from reduced instances of financial loss associated with customer fraud, due to the high standard of secure verification offered by the System. This will result in greater efficiencies, through reduced time and costs associated with investigation and prosecution of fraud events.

Businesses participating as relying parties will also enjoy greater efficiency across their front-end operations and will be able to provide an improved customer experience, as a result of reduced manual handling and wait times. This is likely to benefit a wide range of companies that require customer identity verification, and who are unable to participate in the System as relying parties under the status quo arrangements, such as utility providers, telecommunications companies, banks, insurance providers and more. Economic modelling indicates that new Australian businesses may achieve time savings worth between $22.6 million and $45.3 million a year, simply by using the System to complete business set-up tasks with government entities. The productivity benefits associated with expanded access to the System for *all* kinds of transactions across multiple sectors, including verification of customer identities, would therefore be expected to be many times greater (source: *Economic Benefits of Digital Identity* 2020, KPMG).

(b) Expected costs of regulatory scheme

The proposed regulatory scheme prohibits mandating use of the System, including by relying parties. This means that businesses which seek to use the System will still have to provide alternative options such as paper-based and face-to-face identity verification. The requirement to provide alternative options may mean that businesses are not able to fully realise the potential productivity benefits/time savings discussed above. The scheme would allow, however, for exceptions to this requirement in narrow, clearly defined circumstances (for example, entities which only offer fully online services). It is expected that alternative channels will be chosen by customers for a minority of transactions, due to the predominant and growing popularity of digital channels to interact with services. This means that while existing manual channels will still be available, their lower volume of use will drive costs down compared to having no Digital Identity-enabled option at all.

It is not expected that relying parties will be brought within the provisions of the Privacy Act by this legislation if they are not already required to comply with it – these provisions only apply to onboarded accredited entities. However, when

particularly sensitive types of individual data are involved, the regulatory scheme establishes increased requirements for relying parties in relation to data handling and user safeguards, including obligations to report to the Oversight Authority any breach that affects the integrity of the System, such as a suspected fraud or cyber security incident.

The extent of costs imposed on relying parties as a result of these requirements will depend on the extent to which they differ from practices and systems already in place within individual businesses. For example, businesses which engage in significant data handling may have established practices and processes to comply with these requirements and would therefore not incur additional costs. Furthermore, as with onboarded accredited entities, becoming a relying party is entirely voluntary so businesses which do not expect to gain net benefits from the System are free to not participate.

As is the case for onboarded accredited entity businesses, relying party businesses may also forego access to or ownership over some customer data. For private sector businesses, the aggregation and sale of customer data may present a meaningful commercial opportunity. Using the System may affect an organisation's practical or legal ability to capitalise on such an opportunity. However, as noted above, the extent to which these opportunity costs are experienced by an individual business would be highly dependent on their prior commercial arrangements and service offerings.

As this legislation establishes the framework for a System charging regime, an indirect consequence is that relying parties will face future charges for using services within the System provided by onboarded accredited entities. This would occur in circumstances where these entities seek to recover costs imposed under the charging regime by levying processing or other fees on relying parties. The extent and value of these potential fees will not be prescribed in the primary legislation, but legislation will set a framework within which onboarded accredited entities will operate in a competitive market context. Because of this, it is anticipated that any charges for relying parties will be set at a level that incentivises (or at least does not create a significant barrier to) uptake of System services. Charging practices by onboarded accredited entities would be subject to the standard safeguards applying under relevant competition law (including prohibitions on cartel conduct and

coordinated price-setting). This is expected to ensure relying parties can enter into cost-competitive arrangements with onboarded accredited entities and seek out the most cost-effective arrangements through standard market competition mechanisms. In providing a mechanism for the establishment and detail of the charging regime, the legislation creates the potential for further regulation to be enacted in relation to charging practices between onboarded accredited entities and relying parties.

Overall, the cost implications of this regulatory scheme for businesses wishing to participate in the Program as relying parties are expected to be significantly lower than for onboarded accredited entities because of the lesser regulatory requirements imposed on these participants.

Assessment of net expected benefits

The benefits and costs accruing to businesses as a result of this dedicated regulatory scheme are expected to vary significantly depending on:

- whether a business intends to seek accreditation, or participate as an onboarded accredited entity or as a relying party
- whether a business is already subject to the provisions of the Privacy Act and has processes and infrastructure in place to meet the data handling and security requirements of this regulatory scheme
- the frequency and volume of a business' customer verification requirements in delivering services
- the extent to which a business has already adopted digital options for processing identity verification requests.

Because of these multiple variables, it is challenging to reach a single assessment of the net expected benefits accruing to businesses from this regulatory scheme. However, because participation in the System is voluntary for businesses, it is expected that only those organisations which perceive a net positive benefit – financially and operationally – will do so. In general, it is also expected that the significant benefits accruing to relying parties from increased productivity, faster speed of processing and improved client experience will outweigh the costs associated with the limited regulatory requirements imposed. Similarly, where an organisation which seeks to become an onboarded accredited entity is already subject to the existing provisions of the Privacy Act and the NDB Scheme, it is

expected that the additional benefits accruing through improved efficiency, additional revenue streams and reduced legal risk will outweigh the costs of regulatory compliance.

9.1.3 Government

(a) Expected benefits of regulatory scheme

Option 3 entails the Australian Government playing an ongoing role in the delivery of the Program, as well as in the drafting and enactment of legislation and subordinate regulations supporting its expansion. This option will enable the Government to meet the strategic objectives it has outlined as part of its Digital Transformation Strategy, including a commitment that Australians "… will be able to choose a secure and easy to use Digital Identity to access all digital government services."

All levels of government will enjoy greater efficiency and reduced manual handling in customer operations. This has the potential to benefit a wide range of government entities that frequently require customer identification to provide services. These potential applications are likely to support opportunities for productivity improvements and cost efficiencies at all levels of government.

However, the expansion of the System especially presents an opportunity for the modernisation of public services at a state, territory and local government level. The extent and frequency of individuals' touchpoints with state, territory and local government-provided services means the System – through its enablement of reduced paperwork, faster transactions and improved convenience - will generate significant gains in administrative efficiency. Digital Identity offers a consistent, central mechanism for identity proofing, which will reduce the need for multiple entities to verify an individual's identity. Cost savings will be garnered from a substantially lessened requirement for agency-specific identity, access management services and subsequent support systems.

The use of the System has the potential to support state and territory government services across:

- the registration of births, deaths and marriages
- state and local government licensing regimes

- school and vocational education enrolment
- healthcare, including hospital and ambulance services
- utility services, such as water, gas and power, from state corporations
- collection of state taxes and revenue – for example, payroll tax and property rates.

Further, in interacting with businesses, state and territory governments can streamline the provision of services relating to business registrations, economic support, authorisations and permits, leading to even greater opportunities for cost reductions. These efficiency gains, cost savings and service enhancements would also be available to local governments and their management of various community services. The significant annual volume of transactions requiring identity verification in these areas is expected to generate significant efficiencies for state and local governments which are able to use the System in place of paper-based and face-to-face identity verification.

Governments will also benefit from a reduction in identity fraud as a result of an expanded System, through reduced instances of paying benefits or supplying services to people who are not entitled. In 2018-19, the Department of Social Services reported that its Investigations section had assessed 40 instances of suspected internal and external fraud. The costs associated with such investigations and subsequent action, where that fraud relates to identity, may be mitigated by the System.

Additionally, as legislation will support an expansion of the System to all levels of government, state, territory, local governments and individual Australian Government agencies will save time and costs, as they can reduce investment in their own digital identity platforms or may no longer need to develop their own solutions. The System's automatic de-duplication processes would also present a significant time and cost saving for these additional government entities, who may be required to undertake these data integrity measures manually or using other systems. The extent of this saving for each government entity is difficult to quantify, as it is dependent on the impact of multiple identity accounts linked to one individual (which varies depending on the particular system).

(b) Expected costs of regulatory scheme

Australian Government agencies and governments of all levels may incur costs as a result of a need to transition from or decommission existing digital identity investments and services, where such platforms are under development. However, as the System remains voluntary, this regulatory scheme would not directly drive the decision that leads to these costs – rather, each agency would need to determine whether these costs are outweighed by the benefits of using the Australian Government Digital Identity System.

Australian Government, state and territory governments may incur some costs associated with updating existing legislation, regulation or policies, to ensure alignment with the new regulatory scheme. This may include costs associated with updates for new privacy or security requirements, as well as the flow-on costs of complying with any increased privacy standards. These costs are expected to be limited for most jurisdictions which already have standalone privacy legislation in place, and nil for Government entities since they are already subject to the national privacy regime. They are likely to be greater for South Australia and Western Australia which currently do not have established state-based privacy regimes.

The regulatory scheme's intended leveraging of certain requirements under the NDB Scheme to apply to all participants within the System (including state and territory governments, which currently are not subject to the Scheme), will require entities to monitor data breaches and report these to the Oversight Authority and their own regulator. This new requirement may impose significant regulatory costs at the state and territory levels of government, where the NDB Scheme or a comparable set of obligations do not currently operate. Further, states and territories will be subject to the charging regime, which presents a further potential cost. However, it should be noted that states and territories will be permitted to recover some costs through relying parties who seek to transact with state and territory government onboarded accredited entities.

Assessment of net expected benefits: The expansion of the System to a wider range of Australian Government entities and state, territory and local governments creates the potential for very large productivity and efficiency gains in relation to identity verification. In addition to reducing manual handling of paperwork and freeing up staff resourcing to focus on more complex/meaningful service delivery work, the

System also allows government entities to offer citizens a better service experience. This is expected to generate intangible benefits in relation to citizen satisfaction, staff experience and attachment which cannot be costed but will contribute to the overall benefits delivered by this Option 3.

As with businesses, the expected costs of government compliance with this regulatory scheme will vary depending on the baseline state of entities in relation to their current privacy, data reporting and other information-handling obligations. Given that a majority of government entities are already subject to these obligations in some form, the transition costs and ongoing compliance costs are not anticipated to be significantly different from the status quo at this point in time. However, any state and territory governments participating in the System as onboarded accredited entities, will face new regulatory requirements equivalent to those imposed by the NDB Scheme. Non- Australian Government agencies will also be subject to the System's charging regime, the details of which are still under development however will impact governments acting both as relying parties and onboarded accredited entities.

Overall, these factors are expected to amount to strongly positive net benefits for all levels of government from the expanded agency participation, increased citizen uptake and improved trust in the System enabled by this regulatory scheme.

9.1.4 Community

With legislation facilitating an expansion of the System, this is expected to lead to enhanced uptake and therefore familiarity with digital identity by individuals and businesses. As a result, the community may experience an increase in trust and greater confidence in digital identity and related services. Such trust and confidence is only likely to grow as community exposure to the Program increases, and individuals are able to make more frequent use of the System on a day-to-day basis.

Legislation will enable community organisations to interact with the System, most likely as relying parties. As such, improvements to the speed with which they interact with a wider range of government and private sector entities will result in time and cost savings, as well as increased productivity. Further, community organisations will enjoy greater efficiency in their customer operations and reduced manual handling

where, for example, a housing service provider is required to interact with multiple entities to verify a customer's identity. These time and cost savings are particularly significant where such organisations have access to limited resources in the first instance.

There are likely very limited cost implications for the community from enshrining System principles, governance and requirements in the proposed new regulatory regime. Benefits to the community, including enhanced trust and confidence in the System, will flow from individuals' largely free participation in Digital Identity.

Similarly, where community organisations participate in the System as relying parties, the costs incurred will be limited, as regulatory measures are predominantly focused on onboarded accredited entities. However, it should be noted that decisions surrounding the extent to which costs levied under the charging regime will be passed on are relevant for community organisations. If such organisations are charged for their participation in the System (as relying parties), this may have cost implications for community providers.

Assessment of net expected benefits: There are strongly positive benefits for the community, emerging from the introduction of the regulatory scheme. These include enhanced feelings of trust and confidence across the community in the System and services – which, although not capable of quantification, contribute to the overall benefit to the community under Option 3. Further, community organisations stand to benefit in particular from efficiency gains and reduced manual handling.

While community organisations choosing to participate will be subject to costs levied under the charging regime, costs to community organisations as relying parties, and to the community as a whole, are likely very limited.

9.2 Regulatory impacts

Of all options, Option 3 involves the most significant regulatory costs for the categories of regulated entities, being relying parties, accredited entities and onboarded accredited entities. In order to validate quantification of these costs, the expected impacts have been listed in the following pages of this document, including an initial estimated regulatory cost developed in accordance with Appendix E Regulatory Costs: Methodology and Assumptions, with corresponding consultation

questions in blue boxes. These questions seek information to refine estimates, better understand the impacts of proposed regulatory measures on different entities, as well as validating several underlying assumptions.

In these tables, a complete list of regulatory impacts have been identified within the Exposure Draft package and categorised as below. Only regulatory measures which necessitate some positive action from regulated entities have been included (not, for example, prohibitions on the entity doing something they are unlikely to already be doing). Additionally, regulatory measures such as the Interoperability Obligation (requiring each onboarded entity to interact with all other entities on the System) have not been included, as this is planned to be enabled by the System design and does not require positive activity by regulated entities. Many regulatory requirements include provision for exemptions based upon defined criteria, however to ensure completeness for regulatory costing purposes it is assumed that exemptions will not be granted.

9.2.1 Applications

The application/s that various entities would need to submit under Option 3. Depending on the type of entity, these may include applications for accreditation and/or onboarding. The broad requirements of each step of the application process have been outlined.

9.2.2 Privacy and security obligations

Positive obligations on entities in relation to privacy and security aspects of this Option. These range from positive reporting obligations (e.g. in the event of a data breach), to implementing processes to ensure user consent is obtained at required points. Special requirements attach to some types of regulated entities, such as relying parties that have been approved to receive restricted attributes, and those dealing with biometric information.

9.2.3 Ongoing obligations

The ongoing obligations an entity is subject to as a result of either their connection to the System, or their accreditation under the TDIF. These may include, for example,

annual assessments and reaccreditation-related requirements (if directed by the Oversight Authority).

9.2.4 Administrative

Various administrative requirements of regulated entities under the regulatory scheme including recordkeeping and data retention requirements. These obligations vary as appropriate given the involvement and likely data accessed and used by an entity within the System. It is expected that some administrative requirements included in the regulatory scheme (such as compliance with payment terms) would already be a part of an entity's business-as-usual activities, and therefore would impose no additional regulatory cost (as set out in 'Assumptions' section below).

I am a prospective relying party (non-government)		Consultation question(s)
This means that I would:	Seek to provide a digital service to people with a digital identity, relying upon verified information passed through the System.	N/A
Under this regulatory scheme, I would have to:	**Applications:** 1. Apply online, through a secure online portal, to the Oversight Authority to be onboarded to the System and added to the Register. The application process involves filling out an approved form, including paying a fee, and having an appropriate management authority certify the form. The application for onboarding considers such matters as demonstrated compliance with technical /data rules, security considerations and a fit and proper person test. 2. Apply to the Oversight Authority if I wish to receive sensitive or higher-risk attributes (restricted attributes), rather than the standard (core) attributes under the System. This application must include detail such as justification for requesting the Attribute, information on the relying party's protective security, privacy and fraud control arrangements, a risk assessment, a Privacy Impact Assessment, and data flows showing how the Restricted Attribute will be used. **Privacy and security obligations:** 3. Comply with any Oversight Authority conditions governing when and how I may use or share attributes. 4. If approved to receive restricted attributes, comply with additional privacy/integrity requirements. **Ongoing obligations:** 5. Comply with the legislation's requirement that creation and use of a digital identity through the System is voluntary and entirely by choice. 6. In order to ensure that use of the System remains voluntary, provide my customers with alternative channels for access/interaction to my services. **Administrative:** 7. Notify the Oversight Authority of incidents such as outages, suspected fraud, cyber-security, change of control (within the meaning of the Corporations Act) of a company, change of a service provider /contractor in respect of delivery of any digital identity activities (not labour hire contractors, but service providers providing technical services), and assist with resolution. 8. Inform the Oversight Authority promptly of any changes to my details published on the TDIF System Register.	(3) What is the estimated resource effort required for your entity to comply with the onboarding Application requirements (resource hours /days)? (4) If your entity is likely to apply to receive restricted attributes, what is the estimated resource effort required for it to comply with this application requirements (resource hours/days)? (5) What is the estimated resource effort required for your entity to comply with the Privacy and Security obligations (resource hours/days)? (6) What is the estimated resource effort required for your entity to comply with the Ongoing obligations (resource hours /days)? (7) What is the estimated resource effort required for your entity to comply with the Administrative obligations (resource hours/days)? (8) Are there costs other than staff effort which will be incurred, beyond business-as-usual costs, to comply with the regulations (e.g. capital costs or supplier expenses)? If so, what are these and what is the expected cost?
The regulatory scheme would also require this, however it is assumed that I would already substantially meet or be capable of meeting these requirements in the course of doing business:	1. Comply with payment terms and other related requirements in the rules at the time of onboarding. 2. Comply with relevant statutory requirements, including Privacy Act requirements, relevant to my dealings with information within the System. 3. Have appropriate protective security, privacy and fraud control arrangements in place to prevent information being disclosed to unauthorised third parties. 4. Have and maintain insurance as relevant to my activities in the System.	(9) Is this assumption correct or incorrect? (10) For which of the requirements? (11) If incorrect, how much time/resource effort would it take to comply with this requirement?

Table 3: Estimated regulatory impacts for relying parties (non-government)

Based upon initial calculations, as outlined in Appendix E Regulatory costs: Methodology and assumptions, the regulatory cost ranges of Option 3 for prospective relying parties has been estimated as $4,164-$7,195 in the initial year, and $3,908-$6,720 for every year following that an entity remains as a relying party in the System. (Note: This is the estimated amount it would cost an entity to comply with the proposed regulations, based on the time and labour cost of undertaking the above activities (i.e. it is not a 'fee' or 'charge' to use the System). Sections 6.3, 9.2 and Appendix E provide further detail regarding the methodology by which these estimates have been developed, which is consistent with the Australian Government's Regulatory Burden Measurement Framework. Importantly, this regulatory cost figure does not constitute nor indicate a proposed charge for using the System.) As described below in Section 9.3, the significant benefits to be gained by an entity through expansion and regulation of the System are expected to substantially outweigh these costs of regulatory compliance.

I am a prospective accredited entity (non-government)		Consultation questions
This means that I would:	Be accredited under the Trusted Digital Identity Framework for a particular role (AP, CSP, IDX and/or IDP), but I would not be connected ("onboarded") to the System.	N/A
Under this regulatory scheme, I would have to:	**Applications:** 1. Apply for approval to proceed to the full accreditation process, for the relevant role. The applicant must submit an accreditation schedule with the application and demonstrate to the Oversight Authority that the applicant's facility is sufficiently developed, the applicant has sufficient technical and financial resources and an adequate forward plan available to become an accredited entity. 2. Submit an application for accreditation, demonstrating how the entity meets the fit and proper person test, and its activity /system meets the requirements as set out in the legislation and the TDIF. Applicants must commission (unless exempted) independent assessor to provide reports on the "functional assessments" set out in the TDIF, including protective security, privacy, accessibility and usability. This may include (without limitation), a Privacy Impact Assessment, Security Assessment, penetration testing and Web content guidelines assessment. **Privacy and security obligations:** 1. For an entity not covered by the Privacy Act or a comparable State/Territory law in respect of the personal information they may obtain through the System, bring themselves within the Privacy Act through mechanisms in the Act (currently, this requirement would impact only small businesses in WA and SA, who may not already be subject to privacy legislation unless they have opted in) 2. Provide a copy of statements provided to the Information Commissioner (or, as applicable, the State or Territory privacy authority) under the NDB scheme, to the Oversight Authority at the same time (the legislation does not affect the operation of the NDB scheme, which would apply to all accredited entities once they opt into the Privacy Act) 3. [IDXs only] Implement processes to ensure that your entity does not send any Attributes to a relying party unless/until a user has expressly consented (i.e. by ticking a box on a screen). 4. Comply with prohibitions on the creation of a single identifier for individuals that could be used across a digital identity system. An IDX must create a different identifier for each relying party or IDP connection relating to an individual. 5. If approved to use and share biometric information (IP3 accredited), comply with prohibitions on sending biometric information received through their digital identity system to any third parties not required to perform biometric matching or authentication for the user. 6. If approved to use and share biometric information (IP3 accredited), obtain user's express consent to use their biometric information for specific purposes, and delete biometric information when the purpose for which it was provided is complete. **Ongoing obligations:** 1. If directed by the Oversight Authority, undergo "reaccreditation" if any of the following occur – a cyber security incident, a fraud incident, a serious/repeated breach of a system privacy requirement, or where the accredited entity has changed a service provider/contractor in respect of delivery of any digital identity activities (i.e. service providers providing technical services, not labour hire contractors). 2. Undergo an annual accreditation assessment, demonstrating continued compliance with accreditation rules and requirements. 3. [Identity providers only] Promptly deactivate a User's digital identity if requested by that individual. **Administrative:** 1. Not Applicable.	(12) How long would it take your organisation to comply with the Accreditation Application requirements (resource hours/days)? (13) How long would it take your organisation to comply with the Privacy and Security Obligations (resource hours/days)? (14) How long would it take your organisation to comply with these other ongoing obligations (resource hours/days)? (15) How long would it take your organisation to comply with the Administrative requirements (resource hours/days)? (16) Are there costs other than staff effort which will be incurred, beyond business-as-usual costs, to comply with the regulations (e.g. capital costs or supplier expenses)? If so, what are these and what is the expected cost?
The regulatory scheme would also require this, however it is assumed that I would already meet or substantially	1. Comply with accessible and inclusive website design principles, including compliance with specified accessibility guidelines and standards, use of clear, concise and plain English across all devices and browsers, and undertake useability testing with a range of individuals who require additional accessibility requirements. 2. Comply with existing privacy laws and relevant NDB schemes in your jurisdiction, in respect of personal information collected and disclosed related to a digital identity service	(17) Is this assumption correct or incorrect? (18) For which of the requirements?

meet these requirements in the course of doing business:	3. As an ongoing requirement of accreditation, have arrangements in place covering various topics as set out in the TDIF accreditation rules, including: • Incident management, investigations and monitoring plan (including obligations to contact affected parties) • Protective security, including fraud control plan, and corresponding training • Privacy policy and corresponding training • Disaster recovery and business continuity plans • Personnel security and suitability arrangements • Records management • Risk management • Identity proofing • Authentication credential management.	(19) If incorrect, how much time/resource effort would it take to comply with this requirement?

Table 4: Estimated regulatory impacts for accredited entities (non-government)

Based upon initial calculations, as outlined in Appendix E Regulatory costs: Methodology and assumptions, the regulatory cost ranges of Option 3 for prospective Accredited Entities has been estimated as $5,515-$11,724 in the initial year, and $5,332-$11,468 for every year following that an entity remains as an accredited entity. (Note: This is the estimated amount it would cost an entity to comply with the proposed regulations, based on the time and labour cost of undertaking the above activities (i.e. it is not a 'fee' or 'charge' to use the System). Sections 6.3, 9.2 and Appendix E provide further detail regarding the methodology by which these estimates have been developed, which is consistent with the Australian Government's Regulatory Burden Measurement Framework. Importantly, this regulatory cost figure does not constitute nor indicate a proposed charge for accreditation or using the System. As described below in Section 9.3, the significant benefits to be gained by an entity through expansion and regulation of the System are expected to substantially outweigh these costs of regulatory compliance.

I am a prospective onboarded accredited entity (non-government)		Consultation questions
This means that I would:	Be accredited under the Trusted Digital Identity Framework for a particular role (AP, CSP, IDX and/or IDP), and be onboarded to the System to perform that role.	N/A
Under this regulatory scheme, I would have to:	**Applications:** 1. Apply for approval to proceed to the full accreditation process, for the relevant role. The applicant must submit an accreditation schedule with the application and demonstrate to the Oversight Authority that the applicant's facility is sufficiently developed, the applicant has sufficient technical and financial resources and an adequate forward plan available to become an onboarded accredited entity. 2. Submit an application for accreditation, demonstrating how the entity meets the fit and proper person test, and its activity/system meets the requirements as set out in the legislation and the TDIF. Applicants must commission (unless exempted) independent assessor to provide reports on the "functional assessments" set out in the TDIF, including protective security, privacy, accessibility and usability. This may include (without limitation), a Privacy Impact Assessment, Security Assessment, penetration testing and Web content guidelines assessment. 3. Submit an application for onboarding (note – this may be done as a joint accreditation/onboarding application). The onboarding application considers: demonstrated compliance with technical/data rules, risks to the system, security considerations, fit and proper person test (as for accreditation), additional conditions imposed by the Oversight Authority (e.g. authorising the entity to obtain or disclose a restricted attribute of an individual) and whether entity has entered into an arrangement with the Australian Government. **Privacy and security obligations:** 1. For an entity not covered by the Privacy Act or a comparable state/territory law in respect of the personal information they may obtain through the System, bring themselves within the Privacy Act through mechanisms in	(20) How long would it take your organisation to comply with the Application requirements (resource hours/days)? (21) How long would it take your organisation to comply with the Privacy and Security requirements (resource hours/days)? (22) How long would it take your organisation to comply with the ongoing requirements (resource hours/days)? (23) How long would it take your organisation to comply with the Administrative requirements (resource hours/days)? (24) Are there costs other than staff effort which will be incurred, beyond business-as-usual costs, to comply with the regulations (e.g. capital costs or supplier expenses)? If so, what are these and what is the expected cost?

	this Act (currently, this requirement would impact only small businesses in WA and SA, who may not already be subject to privacy legislation unless they have opted in). 2. Provide a copy of statements provided to the Information Commissioner (or, as applicable, the relevant State or Territory privacy authority) under the NDB scheme, to the Oversight Authority at the same time (the legislation does not affect the operation of the NDB scheme, which would apply to all accredited entities once they opt into the Privacy Act). 3. [IDXs only] Implement processes to ensure that your entity does not send any attributes to a relying party unless/until a user has expressly consented (i.e. by ticking a box on a screen). 4. Comply with prohibitions on the creation of a single identifier for individuals that could be used across a digital identity system. An onboarded accredited entity may not generate a new identifier to refer to a user and pass that same identifier to more than one other onboarded accredited entity or relying party. 5. If approved to use and share biometric information through the System (IP3 accredited), comply with prohibitions on sending biometric information received through the system to any third parties not required to perform biometric matching or authentication for the user. 6. If approved to use and share biometric information through the System (IP3 accredited), obtain user's express consent to use their biometric information for specific purposes, and delete biometric information when the purpose for which it was provided is complete. 7. Comply with prohibitions on collecting, using and disclosing information about a user's behaviour on the System, except to verify their identify and assist them in receiving a service, support an identity fraud management function, improve the performance and useability of the system, and other authorised purposes. Prohibited purposes include: unrelating marketing and speculative profiling. **Ongoing obligations:** 1. If directed by the Oversight Authority, undergo "reaccreditation" if any of the following occur – a cyber security incident, a fraud incident, a serious/repeated breach of a system privacy requirement, a change of control occurs in the entity, or where the onboarded accredited entity has changed a service provider/contractor in respect of delivery of any digital identity activities (i.e. service providers providing technical services, not labour hire contractors). 2. Undergo an annual accreditation assessment, demonstrating continued compliance with accreditation rules and requirements. 3. Interact with all entities on the System where requested to do so by another entity using the System. This includes, IDXs being connected to each other, IDPs competing to provide their services to any relying party, unless exempted (Interoperability obligation). 4. Comply with the legislation's requirement that creation and use of a digital identity through the System is voluntary and entirely by choice. 5. [IDPs only] Promptly deactivate a user's digital identity if requested by that individual. **Administrative:** 1. Keep records of the kind and for the period as prescribed by rules, which will not exceed 7 years unless specified circumstances apply. 2. Notify the Oversight Authority of incidents such as suspected fraud, cyber-security, change of control (within the meaning of the Corporations Act) of a company, change of a service provider/contractor in respect of delivery of any digital identity activities (not labour hire contractors, but service providers providing technical services).	
The regulatory scheme would also require this, however it is assumed that I would already meet or substantially meet these requirements in the course of doing business:	1. Comply with accessible and inclusive website design principles, including compliance with specified accessibility guidelines and standards, use of clear, concise and plain English across all devices and browsers, and undertake useability testing with a range of individuals who require additional accessibility requirements. 2. As an ongoing requirement of accreditation, have arrangements in place covering various topics as set out in the TDIF accreditation rules, including: a. Incident management, investigations and monitoring plan (including obligations to contact affected parties) b. Protective security, including fraud control plan, and corresponding training c. Privacy policy and corresponding training	(25) Is this assumption correct or incorrect? (26) For which of the requirements? (27) If incorrect, how much time/resource effort would it take to comply with this requirement?

	d. Disaster recovery and business continuity plans e. Personnel security and suitability arrangements f. Records management g. Risk management h. Identity proofing i. Authentication credential management. 3. In relation to cyber security, take steps to improve systems and address vulnerabilities, provide staff training in relation to identifying and dealing with cyber security incidents, develop policies and mechanisms for assisting and coordinating responses to a cyber security incident, and comply with requirements for collecting and collating information about identity theft. 4. Have and maintain insurance as relevant to my activities in the System.	

Table 5: Estimated regulatory impacts for onboarded accredited entities (non-government)

Based upon initial calculations, as outlined in Appendix E Regulatory costs: Methodology and assumptions, the regulatory cost ranges of Option 3 for prospective onboarded accredited entities has been estimated as $7,378–$17,019 in the initial year, and $7,012–$16,435 for every year following that an entity remains an onboarded accredited entity in the System. (Note: This is the estimated amount it would cost an entity to comply with the proposed regulations, based on the time and labour cost of undertaking the above activities (i.e. it is not a 'fee' or 'charge' to use the System). Sections 6.3, 9.2 and Appendix E provide further detail regarding the methodology by which these estimates have been developed, which is consistent with the Australian Government's Regulatory Burden Measurement Framework. Importantly, this regulatory cost figure does not constitute nor indicate a proposed charge for using the System. As described in Section 9.3, the significant benefits to be gained by an entity through expansion and regulation of the System are expected to substantially outweigh these costs of regulatory compliance.

9.3 Likely net benefit

The overall likely net benefit of Option 3 can be determined with reference to the costs and benefits identified for each stakeholder group – individuals, businesses (as onboarded accredited entities and relying parties), government and community.

For individuals, there are significant direct and indirect benefits that will flow from the establishment of a dedicated regulatory scheme through legislation, including time and cost savings, and a reduced risk of identity fraud and misuse of personal information. Given the minimal costs to be borne by individuals under this option, the balance of net benefits for individual Australians is expected to be strongly positive.

For businesses, the impacts will vary depending on various factors, including intended involvement as an onboarded accredited entity or relying party, and extent of existing compliance with the Privacy Act, data handling and security procedures. These variables make it difficult to assess the net expected benefits for businesses in aggregate under Option 3. However, voluntary participation in the System means it is likely that only those organisations which perceive a net positive benefit will choose to participate. Further, participation as a relying party will see businesses benefit from increased productivity, faster speed of processing and improved client experience. For onboarded accredited entity businesses whose practices already demonstrate alignment with the regulatory scheme's requirements, it is expected that the additional benefits accruing through improved efficiency, additional revenue streams and reduced legal risk will outweigh the costs of regulatory compliance.

Australian Government, state, territory and local governments are likely to benefit from significant productivity and efficiency gains across their identity verification practices, allowing government entities to offer Australians a more positive service experience. While citizen satisfaction, staff experience and attachment cannot be costed, these factors will contribute to the overall benefits of Option 3. While the expected costs of government compliance will vary across entities, the transition and ongoing compliance costs of Option 3 are not anticipated to be significantly different from the status quo. These factors indicate strongly positive net benefits for government from the expanded agency participation, increased citizen uptake and improved trust enabled by the proposed regulatory scheme.

The community will benefit from Option 3, including through enhanced feelings of trust and confidence in System services. Community organisations which are enabled to participate are also likely to see improvements in their productivity, potentially offset slightly by costs levied under the charging regime.

Overall, there are significant anticipated benefits to individuals, businesses, governments and the broader economy from the expansion of the System enabled by this legislation. The policy decision to limit the focus of the regulatory scheme to onboarded accredited entities, accredited entities and relying parties means regulation impacts will be felt only by a subset of those who are expected receive these benefits. Entities can assess the benefits and associated costs of participation in the System framework as an onboarded accredited entity, and voluntarily choose to undergo the accreditation process if this balance of costs and benefits is considered to be favourable.

Establishment of a dedicated regulatory scheme through legislation is the only option which supports expansion of the System to a wider range of public and private sector services, particularly non-Australian Government relying parties and onboarded accredited entities able to charge under a legislative framework. The economy-wide benefits of time saved (individuals), productivity (businesses, government and community) and security (all stakeholders) are expected to continue to grow as more entities can access the System.

Consultation question

(28) Overall, are the impacts of Option 3, and the estimated costs, accurately described as related to your entity? Are there any other impacts (negative, positive or neutral) not mentioned above?

10 Consultation to date and future roadmap

10.1 Purpose and objectives

Since the Program's commencement, a continuous and broad-based consultation approach has engaged stakeholders at all levels, on topics from technical design to operation to governance. Stakeholders consulted to date include government, regulatory entities, jurisdictions, privacy advocates, compliance scheme representatives, corporate Australia, small business, peak bodies representing end-users and the general public, as shown in Figure 3.

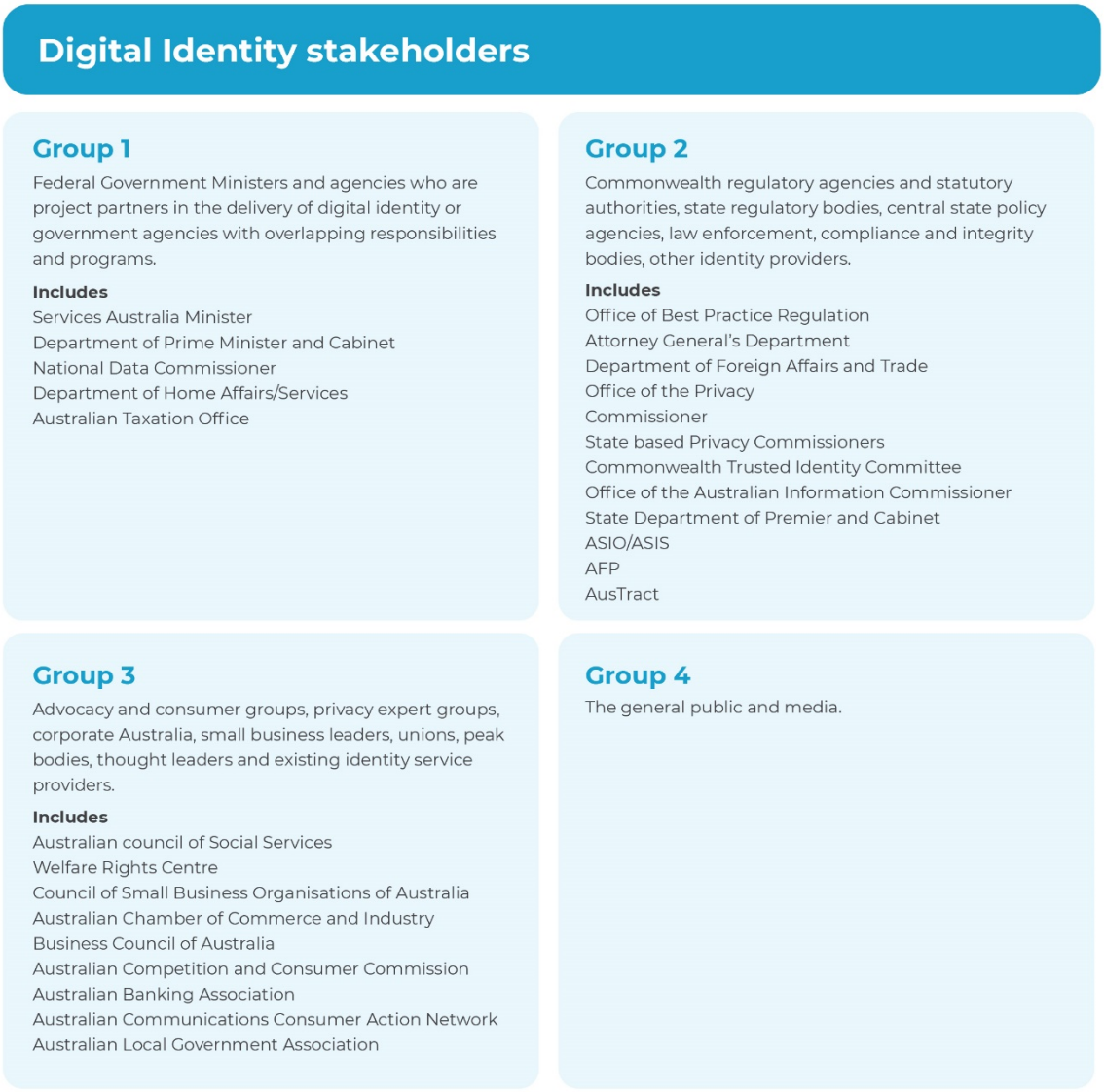


Figure 34567: Australian stakeholders potentially impacted by the System and consulted by the Program

Australia also engages heavily with international stakeholders and counterparts in digital identity and is recognised as a leader in this space. The Australian Government is involved in trade negotiations with several countries to achieve mutual recognition of identity systems. A Memorandum of Understanding has been established with the Smart Nation and Digital Government Office of Singapore, with a roadmap to the goal of system interoperability with Singapore's national digital identity system. Australia signed a mutual recognition agreement and roadmap with New Zealand in 2020, and is closely collaborating to ensure future policy and system interoperability as both countries develop legislation. Negotiations are also in progress with the UK and Canada. Additionally, Australia is now leading the DGX Digital Identity Working Group - an international working group with members from

the UK, Finland, Singapore, Canada New Zealand and the World Bank - dedicated to achieving digital identity policy interoperability across international borders. The DTA continues to work with the Australian Government and with similar agencies around the world to identify future opportunities for digital identity interoperability and mutual recognition with other countries.

As the System expands to become a whole-of-economy solution, supported by appropriate regulation, this domestic and international engagement will continue and increase. The consultation approach to date, and future activities described in this section, seek to fulfil two primary objectives:

- Ensuring that stakeholder views are sought and considered throughout the regulatory development and assessment process
- Validating the impacts (financial and otherwise) of any proposed regulatory action on affected stakeholders.

The consultation plan recognises that digital identity is a complex concept, some aspects of which may not be well understood by the community, involving highly sensitive topics such as privacy and information security. As regulatory approaches continue to be pursued, a plan is in place to ensure that broad-ranging perspectives will inform the development of policy positions, and allow the identification of any unintended consequences.

10.2 Consultation process to date

Consultation has been a key focus since the commencement of the Program, to ensure that the System design, operation and governance considers and accommodates stakeholder views. Since 2015, the DTA has been engaging with the Australian public to build a System that is aligned with community expectations. The broad range of consultations conducted to date by the Program are listed at Appendix D Previous . This consultation has occurred through a variety of channels (including in person, through interactive webinars, surveys, and public submissions).

These program-wide consultations have been supplemented by targeted engagement on matters that are particularly sensitive or complex, such as privacy and consumer safeguards, conducted both by Government directly and (in the case of Privacy Impact Assessments, for example) by independent firms. Various

stakeholders have been specifically engaged on privacy and consumer related matters, including private sector representatives (i.e. payments, banks), academics and advocacy groups, state and territory Ombudsman entities and privacy commissioners. This iterative consultation strategy has served to validate the identified problems, gauge stakeholder views on areas for potential regulation and lay the foundation for broader public consultations.

In November 2020, a public consultation paper was released on Digital Identity legislation. This paper sought government, community, industry, and individual views on the scope, nature and extent of possible government regulation of the System. Supporting the release of the public consultation paper were five webinars conducted to ensure full understanding of the Program's context, and to encourage submissions. These webinars were attended by 110 stakeholders. A total of 44 submissions were received through this process - 16 from state and territory governments, 20 from the private sector (including industry associations) and 8 from individuals and consumer groups. On 12 February 2021, a consultation synthesis report was published summarising key messages, themes and outcomes of this public consultation process. The synthesis report outlined near-uniform agreement on the immense value of the System, and on some level of legislation to govern that System. However, there were differing views on the content and scope of legislation, including which measures should be legally entrenched and which should remain as policy or operational guidance.

The next stage of legislation-specific consultation occurred in June 2021, with release of a Digital Identity legislation position paper providing updated assessments of key policy positions and the nature of potential regulation. The position paper remained open for comment for 5 weeks, with a total of 66 submissions received, and was supplemented by a series of targeted events including 2 roundtables – held on 1 July 2021 for the Australian Institute of International Affairs (AIIA), and 13 July 2021 for the Australian Society for Computers and the Law (AUSCL) respectively. The roundtables saw participation of around 120 stakeholders in total. Other targeted consultation events that occurred during July included a series of Q&A sessions held for the banking and government sectors. In total, these sessions involved participation of around 21 stakeholders.

10.2.1 Outcomes and themes of consultation to date

Each stage of consultation has directly influenced and shaped Program activity – both substantive decisions and planning the future consultation roadmap. In particular, the public consultation paper round, occurring in November to December 2020, elicited several high-level outcomes and themes across different stakeholder groups (34 of the 44 submissions received that agreed to make their feedback public, can be found on the Digital Identity website). These outcomes formed the focus of targeted consultations with critical stakeholders that occurred in early 2021. The subsequent position paper highlighted areas where stakeholder input led to reconsideration of policy and regulatory positions. These changes in policy positions and other considerations have been incorporated into the drafting of the Exposure Draft package accompanying this RIS. Several select examples of how consultation has shaped Program action are set out below.

Consultation Round	Findings/Themes	Impact on Program Activity
Targeted consultation with Australian Government agencies	**Interoperability with other Systems** Strong suggestions made that key principles and concepts of other countries that have implemented Digital ID systems across government and in private sector, such as Sweden, Argentina, Estonia and the UK, be considered in legislative development.	Program initiated follow up research on the operation of digital identity systems across international examples. Key areas of research include what has been done well in those Systems, what the Program can learn as a result and how those Systems have engaged within their countries. This research led to consideration of the potential interoperability of the System (a topic that was identified for targeted consultation at the time). A new interoperability obligation was introduced, clarifying the expectation of how entities would interact.
Public consultation paper round	**Consistency of laws** During the public consultation paper rounds, feedback received from states in particular querying how equivalence between state and territory legislation and the Privacy Act would be measured.	The Program's original position that legislation would allow state and territory entities to participate in the System as onboarded accredited entities where their legislation offers equivalent levels of privacy protection to the Privacy Act was consequently adjusted. The revised position does not require state and territory legislation to be equivalent to the Privacy Act per se, and instead requires that it meet the three broad criteria borrowed from the Data Availability and Transparency (DAT) Bill. The model used in this bill received support in the Program's recent cross-jurisdictional consultation sessions.

Public consultation paper round	**Privacy and other safeguards** Wide support for additional privacy safeguards to be embedded into a regulatory framework. Further, particular interest was received around consumer protections on single identifiers, consent requirements, opt-out functionality and Biometric Information.	The consultation paper's original position explored the possibility of introducing a System-specific privacy regime, including the use of Digital Identity-specific definitions and terminology. Approach was then amended to leverage, to the greatest extent possible, existing privacy frameworks. While most of the safeguards proposed in the consultation paper were retained, further details about how certain proposed protections were developed. These include: A greater ability for state and territory governments participating in the System as onboarded accredited entities to adhere to local privacy legislation The addition of new safeguards on biometrics and profiling.
Public consultation paper round	**Liability and redress framework** Stakeholders broadly supported the concept of a liability and redress framework, with a range of views received on the extent to which participants should be liable for losses suffered by others under the System. The consensus view was that a clear and fair liability framework would be important, and the addition of appropriate mechanisms for non-financial redress to be in the regulatory scheme was further supported.	The framework is now further progressed, leveraging consultation input received. The position as set out in the Exposure Draft package is that a statutory contract will exist between onboarded accredited entities and relying parties on the System, giving participants the right to seek loss or damages where another participant has breached the System's rules.

Table 6: Examples of previous consultation shaping Program actions and positions.

10.3 Future consultation roadmap

The release of this RIS and the Exposure Draft package is the next stage in this broad-reaching consultation process. The outcomes of consultation on these latest Program documents will continue to shape future regulatory policy development.

Release of an Exposure Draft package, in addition to preceding "summary" content such as the Position Papers, provides full transparency to the public on the nature and detail of proposed regulations. The public release of this RIS will enable

regulatory impacts of measures under consideration to be tested with stakeholders. This stage of consultation provides another opportunity for all impacted stakeholders to understand the detail of what is being proposed and have their say on the measures themselves (through the Exposure Draft package) and their regulatory impacts (through this RIS).

Even after the Draft Exposure package of documents become law, it is not envisaged that consultation would cease on the System and its regulation. The Bill mandates consultation for any legislative instruments issued in the future (beyond the baseline level of consultation on any legislative instrument required by the *Legislation Act 2003* (Cth)). Additional consultation obligations, including a public notice process, are also mandated before the making of additional TDIF accreditation rules and data standards. These proposed legislative measures ensure stakeholder views will continue to be considered and incorporated in the System regulatory regime as it evolves in the future.

11 Best option from those considered

The preceding analysis demonstrates that 5.3 Option 3: Dedicated legislation to establish new regulatory scheme is the most suitable of those considered.

The Murray report identified the need for a whole-of-economy digital identity solution, which would help transform service delivery in Australia and generate significant opportunities for the creation of new economic value. As this RIS has outlined, a whole-of-economy solution cannot be realised unless the System is able to facilitate connections between state, territory and private sector services, driving significantly expanded uptake. Option 3 is the only option capable of facilitating this expansion.

Section 4 of this RIS identified the objectives of government action in relation to Digital Identity. These objectives align with, and seek to address, the problem areas discussed in Section 3, which currently inhibit the System's ability to operate as a whole-of-economy solution. As demonstrated by the table below, establishing a dedicated regulatory scheme supports each of these policy objectives and, in turn, comprehensively addresses the problems identified through this RIS.

Problem area	Policy objective	Why Option 3?
1 **No legal basis for participation of non- Australian Government agencies as relying parties, nor for a charging framework**	Government action enables expansion of the System to include non-Australian Government agencies as relying parties, and providing a legal basis for charging by onboarded accredited entities (Australian Government and non-Australian Government), maximising the benefits.	The introduction of a dedicated regulatory scheme under Option 3 will directly address this issue by providing the requisite statutory authority for the System's expansion and for charging, enabling full uptake by non-Australian Government relying parties and onboarded accredited entities. Options 1 and 2 cannot address existing barriers to non-Australian Government participation, as they do not entail the passing of primary legislation providing legislative authority to enable expansion. Therefore, only under Option 3 can the System's whole-of-economy benefits be realised.
2 **Lack of trust in System's privacy and security safeguards.**	Government action enhances community confidence, trust and clarity regarding the Program's privacy and security safeguards.	Option 3 addresses this problem in several ways: A dedicated regulatory scheme will offer a consistent approach to privacy and consumer protections, across all jurisdictions, including some not currently covered by the Privacy Act. The regulatory scheme can be used to supplement current privacy and consumer protections with System-specific laws, for example prohibitions on data commercialisation and relating to biometrics.

Problem area	Policy objective	Why Option 3?
		The implementation of a legislative governance framework will also support enforcement practices. Stakeholder consultation has highlighted Australians' desire for a consistent set of privacy and security safeguards, which can only be offered by a dedicated regulatory scheme. Option 1 offers no avenue for improved clarity and greater public confidence in the System. While Option 2 may, to some degree, improve trust in the System's privacy and security safeguards, it can only do so within the existing general legislative framework and cannot address any identified gaps.
3 **Interim, non-legislative governance framework.**	Government action enhances community confidence, trust and clarity in the integrity, permanence and rigor of the System's governance.	The introduction of a permanent Oversight Authority through Option 3 will legally enshrine the System's enforceability, transparency, independence and accountability, providing greater certainty for all participants. With legislated powers and functions, the Oversight Authority will strengthen protections for participants in the System, support the System's integrity and longevity, and substantially increase the overall rigour offered by current governance arrangement. Under Options 1 and 2, the System would continue to operate under an interim, non-legislative governance framework, which may lead to low levels of trust and confidence. Therefore, only Option 3 can address the government's policy objectives by enhancing trust and reliance.

Table 7: Option 3 alignment with policy objectives and problem areas

Option 3 also presents the strongest opportunity for enhancing alignment with the five guiding principles of the System, discussed in Section 3.2.3 Interim, Non-Legislative Governance Framework: choice, consent, privacy, security and integrity. For example:

- **Choice and consent**: A dedicated regulatory scheme will ensure participation in the System remains voluntary, making certain that individuals consent to their information being collected in connection with the System. For those who do wish to participate, Option 3 will enable and incentivise the participation of a wider range of both public and private sector identity providers as well as a more diverse range of relying parties. As a result, user choice be both legally enshrined and strengthened in practice as a central component of the System.

- **Privacy, security and integrity:** Option 3 offers a consistent approach to privacy protections across all jurisdictions, supported by the legally enshrined enforcement and compliance powers of the Oversight Authority. This permanent governance arrangement will afford individuals avenues for recourse where data breaches occur, as well as ensuring enduring compliance with transparency and accountability mechanisms. Further, security safeguards embedded in the dedicated regulatory scheme will instil greater user trust and confidence in the System, with the likely outcome of increasing uptake.

Option 1 will continue to secure the significant benefits currently available to individuals and businesses using the System. However, by not addressing the obstacles to expansion, it represents a foregone opportunity to maximise these benefits and further enhance the five principles of the System. Individuals would be deprived of the additional choice that would come with System expansion, and legally enshrined accountability, independence and transparency mechanisms. Similarly, Option 2 offers limited opportunity for furthering these principles. Consent and integrity may benefit from slightly strengthened accountability and transparency mechanisms, but without the force of government regulation. Safeguards and avenues for recourse would not be supported by a consistent dedicated regulatory framework established through primary legislation.

As described in Section 9.2 Regulatory impacts, the regulatory scheme's focus on onboarded accredited entities, accredited entities and relying parties means regulatory costs will be felt by a small subset of stakeholders. These entities can assess their ability to meet the regulatory costs of participation and voluntarily choose to undergo the accreditation or onboarding process if this is expected to lead to positive revenue outcomes through the delivery of new or expanded services.

Without a dedicated regulatory scheme, the identified problem areas cannot be addressed, the policy objectives cannot be met, and stakeholders will not experience, to the full extent, the benefits described above. Beyond this, the Australian economy's realisation of the significant economic value of an expanded System would be constrained and compromised.

Although it is the best option from those considered, Option 3 is not, however, without risks. As discussed in Section 4.4 Constraints and barriers to government intervention, there is a risk that Australian Government regulatory action in this space

may be misconstrued or viewed with suspicion and mistrust. The Program is well equipped to monitor and manage this risk, through its established communication forums and its consultation approach. The risk profile associated with this preferred Option 3, and mitigations, are summarised in the following section.

12 Implementation of selected option

12.1 Implementation approach

Effective implementation of the dedicated regulatory scheme will be critical to ensuring Option 3's full benefits can be realised. Implementation planning is currently under way, ensuring that should the Exposure Draft Bill be passed, the dedicated regulatory scheme can be established efficiently and effectively. Implementation of these regulatory measures will not occur in a silo, but will be delivered alongside other streams of ongoing Program implementation effort including strategy, customer experience, architecture, policy, communications and engagement.

Noting that proposed regulatory measures are not yet finalised, with further changes still possible as a result of this public consultation, implementation planning is being conducted in an agile manner. Whilst the proposed legislation provides broad parameters, the Program is operating flexibly within these parameters to ensure that the implementation solution is designed in a way that meets user and other stakeholder needs. Continuing focus areas for implementation planning include:

- cross-Australian Government engagement on the establishment, structure and operating model of the permanent Oversight Authority
- engagement with bodies such as the Information Commissioner and state/territory Privacy Commissioners, on the legislation's potential impact on their activities (including identifying and addressing any unintended consequences)
- further development of the additional instruments, rules, policy documents and other artefacts that will form part of the regulatory ecosystem. These are expected to cover subject matter including the charging framework.

A more detailed summary of implementation progress will be included in the final RIS, with the implementation approach finalised prior to the introduction of legislation to Parliament.

12.2 Implementation challenges and risks

Whilst Option 3 has been determined the most suitable from those considered, it is not without challenges and risks. These are outlined below, including an explanation of how they are being monitored and accommodated within the Program's implementation approach.

No.	Challenge/risk	Likelihood	Consequence	Management
1	Potential for regulation to be misunderstood, or distrusted, leading to low confidence levels and low uptake of Digital Identity.	High	Severe	Clear and strategic communication to the Australian community about the regulatory scheme's purpose and its safeguards (including prohibition on single identifier and in-built consent requirements). The Program's ongoing consultation process and transparency about the intent of regulation (including this stage of releasing an Exposure Draft package) is designed to manage this risk.
2	The compliance/ enforcement/ governance aspects of Option 3 may have a significant impact on other Government entities, including unintended consequences.	High	Serious	Whilst DTA is ultimately responsible for design and delivery, the Program has adopted an agency partnership model from its commencement, drawing on senior executives within partner agencies to seek alignment and agreement on the priorities and approach to achieve the vision. This approach continues, and is supplemented by targeted engagement on matters such as the establishment of the Oversight Authority, and impacts on other entities fulfilling a specific role under the proposed legislation such as the Information Commissioner.
3	There are divergent views on the System and the nature/scope of proposed regulation, meaning that not all stakeholders will be satisfied with the final positions taken.	High	Serious	It is acknowledged that the final form of the regulatory scheme is unlikely to be acceptable to all stakeholders. At every stage of its broad-based, ongoing consultation, the Program has been fully transparent with stakeholders on its policy positions and reasoning, and has amended many of its positions as a direct result of stakeholder feedback. Whilst all stakeholders may not be satisfied with the final position, the impact of this can be mitigated by continuing to demonstrate transparency regarding

No.	Challenge/risk	Likelihood	Consequence	Management
				decision-making, and a genuine willingness to consult. Additionally, as set out in Section 10 above, consultation does not cease following the commencement of the regulatory scheme, with stakeholders still in a position to influence future development of the regulatory framework.
4	Even after commencement of the regulatory scheme, some detail may not be available due to the ongoing development of supplementary legislative instruments, rules and policies.	High	Serious	The dedicated regulatory scheme in Option 3 envisages a structure where principles and content unlikely to change is contained in primary legislation, whereas other detail including technical and charging information (which will need to evolve over time) is set out in supplementary instruments and artefacts. This means that the regulatory scheme at the point of its commencement may not contain all details impacting System participants. Whilst this is a necessary structure to "future-proof" the regulatory regime, it can lead to uncertainty about the impact of future changes. The Exposure Draft package includes two sets of rules for public consultation. In addition, the legislation mandates consultation on all future legislative instruments and key TDIF artefacts to ensure the potential impacts (intended and unintended) are identified prior to introducing any change.
5	Management of dependencies such as the Australian Government's ongoing Privacy Act review.	Medium	Serious	Ongoing Australian Government regulatory initiatives such as the Privacy Act review have the potential to impact this proposed regulatory structure. Close consultation has occurred and will continue with this review to leverage outcomes and ensure no conflicts in regulatory measures or objectives.

Table 8: Challenges and risks of implementation of Option 3

12.3 Ongoing monitoring of implementation effectiveness

There are various measures built into the draft legislation which provide for regular monitoring of the implementation of a dedicated System regulatory scheme, and its ongoing effectiveness. These include:

- requiring that the Information Commissioner include information on its functions and powers in relation to the System as part of its annual report tabled under s46 of the *Public Governance, Performance and Accountability Act 2013* (Cth)
- for transparency and further enshrining independence, the Exposure Draft Bill requires the Oversight Authority to prepare an Annual Report to be tabled in Parliament. The report will report separately on the operation of the System and the accreditation scheme, with – at a minimum – details of number of applications, approvals and fraud and cyber security incidents and responses to fraud and cyber security incidents, as well as other matters as notified by the Minister to the Oversight Authority
- the legislation also provides for a review of the Bill /Act in two years from the date of its commencement.

Additionally, as set out in Section 10.3 Future consultation roadmap the legislation includes mandated consultation on proposed changes to regulation, including the issuance of new legislative instruments. This will provide an effective way of monitoring the effectiveness of Option 3 as the regulatory ecosystem evolves over time.

Overall, the above measures provide a legislative guarantee that the effectiveness of Option 3 will continue to be monitored and evaluated against its objectives, even after the implementation period has concluded.

13 Consultation questions and next steps

The questions on which submissions are sought, as distributed throughout this document, are consolidated below.

(1) Are the impacts of Option 1 accurately described as related to your entity? Are there any other impacts (negative, positive or neutral) of the System continuing without regulation, that are not mentioned above?
(2) Are the impacts of Option 2 accurately described as related to your entity? Are there any other impacts (negative, positive or neutral) not mentioned above?

To prospective relying parties (non-government):

(3) What is the estimated resource effort required for your entity to comply with the onboarding Application requirements (resource hours/days)?
(4) If your entity is likely to apply to receive restricted attributes, what is the estimated resource effort required for it to comply with this application requirements (resource hours/days)?
(5) What is the estimated resource effort required for your entity to comply with the Privacy and Security obligations (resource hours/days)?
(6) What is the estimated resource effort required for your entity to comply with the Ongoing obligations (resource hours/days)?
(7) What is the estimated resource effort required for your entity to comply with the Administrative obligations (resource hours/days)?
(8) Are there costs other than staff effort which will be incurred, beyond business-as-usual costs, to comply with the regulations (e.g. capital costs or supplier expenses)? If so, what are these and what is the expected cost?
(9) Is this assumption correct or incorrect?
(10) For which of the requirements?
(11) If incorrect, how much time/resource effort would it take to comply with this requirement?

To prospective accredited entities (non-government):

(12) What is the estimated resource effort required for your entity to comply with the onboarding Application requirements (resource hours/days)?
(13) What is the estimated resource effort required for your entity to comply with the Privacy and Security obligations (resource hours/days)?
(14) What is the estimated resource effort required for your entity to comply with the Ongoing obligations (resource hours/days)?
(15) What is the estimated resource effort required for your entity to comply with the Administrative obligations (resource hours/days)?
(16) Are there costs other than staff effort which will be incurred, beyond business-as-usual costs, to comply with the regulations (e.g. capital costs or supplier expenses)? If so, what are these and what is the expected cost?
(17) Is this assumption correct or incorrect?
(18) For which of the requirements?
(19) If incorrect, how much time/resource effort would it take to comply with this requirement?

To prospective onboarded accredited entities (non-government):

(20) What is the estimated resource effort required for your entity to comply with the onboarding Application requirements (resource hours/days)?
(21) What is the estimated resource effort required for your entity to comply with the Privacy and Security obligations (resource hours/days)?
(22) What is the estimated resource effort required for your entity to comply with the Ongoing obligations (resource hours/days)?
(23) What is the estimated resource effort required for your entity to comply with the Administrative obligations (resource hours/days)?

(24) Are there costs other than staff effort which will be incurred, beyond business-as-usual costs, to comply with the regulations (e.g. capital costs or supplier expenses)? If so, what are these and what is the expected cost?
(25) Is this assumption correct or incorrect?
(26) For which of the requirements?
(27) If incorrect, how much time/resource effort would it take to comply with this requirement?
(28) Overall, are the impacts of Option 3, and the estimated costs, accurately described as related to your entity? Are there any other impacts (negative or positive) not mentioned above?

Persons and entities wishing to make a submission on the questions above can do so using the relevant Response Form at www.digitalidentity.gov.au/have-your-say. In addition to the above, those making a submission will also be asked a series of general questions about the entity on whose behalf they are responding, location, sector and intended role/s in the System. Please also head to www.digitalidentity.gov.au/have-your-say to provide input on any other non-regulatory impact matters, including Government's proposed policy positions.

Your input will inform the final version of this RIS, which will include validated quantitative analysis of each option's regulatory impacts. In accordance with government guidelines, the Final RIS will be published by the Office of Best Practice Regulation on or before the date on which the legislation is introduced to Parliament.

Appendix A – Glossary

The glossary below highlights key terms, acronyms, and their definitions, as used in this document. Unless otherwise stated, terminology is consistent with the Digital Identity Program Glossary which can be accessed at https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/digital-identity-legislation-position-paper/2-glossary-of-terms.

Term	Definition
Access Card initiative	The Australian Government provided details of a health and social services Access Card in the 2006/2007 budget. The project is more formally known as the 'Health and Social Services Smart Card initiative'. The Access Card was a proposed Australian Government non-compulsory electronic identity card. The scheme was to be phased in over two years, beginning in 2008, but the project was terminated in November 2007.
APP entities	The Privacy Act imposes obligations on 'APP entities'. An APP entity is, generally speaking: an agency (largely referring to a federal government entity and/or office holder) or an organisation (which includes an individual, body corporate, partnership, unincorporated association, or trust).
Australian Consumer and Competition Commission (ACCC)	The Australian Competition and Consumer Commission (ACCC) is an independent Commonwealth statutory authority whose role is to enforce the *Competition and Consumer Act 2010* and a range of additional legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians.
Australian Government Agencies Privacy Code (the Code)	The Australian Government Agencies Privacy Code (the Code) was registered on 27 October 2017 and commenced on 1 July 2018. The Code applies to all Australian Government agencies subject to the Privacy Act 1988 (except for Ministers. It is a binding legislative instrument under the Act. The Code sets out specific requirements and key practical steps that agencies must take as part of complying with Australian Privacy Principle 1.2 (APP 1.2). It requires agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management across all Australian Government agencies.
Australian Law Reform Commission (ALRC)	The Australian Law Reform Commission is an Australian independent statutory body established to conduct reviews into the law of Australia. The reviews, also called inquiries or references, are referred to the ALRC by the Attorney-General for Australia.
Australian Privacy Principles (APPs)	The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the Privacy Act 1988. They apply to any organisation or agency the Privacy Act covers. There are 13 APPs and they govern standards, rights and obligations around: the collection, use and disclosure of personal information, an organisation or agency's governance and accountability, integrity and correction of personal information, and the rights of individuals to access their personal information.

Biometric information (Biometrics)	Information about any measurable biological or behavioural characteristics of a natural person that can be used to identify them or verify their identity, such as face, fingerprints and voice. (Under the Privacy Act 1988, biometric information is considered as sensitive information, which provides additional obligations on organisations.)
Council of Australian Government (COAG)	The Council of Australian Governments (COAG) is the peak intergovernmental forum in Australia. It initiates, develops and monitors policy reforms of national significance which require co-operative action by Australian governments.
COVID-19	Coronavirus disease 2019 (COVID-19) is a contagious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). The first case was identified in Wuhan, China, in December 2019. It has since spread worldwide, leading to an ongoing pandemic.
Digital Government Exchange (DGX)	The Digital Government Exchanges (DGX) are events held for international public sector leaders with deep interest in the use of Smart Technologies in delivering government services to citizens and businesses. It sees attendees from leading digital governments of Denmark, Estonia, Israel, Korea and New Zealand among others, coming together for discussions on issues facing Smart Cities and opportunities for growth through technology.
digital identity	Unless otherwise stated*, "digital identity" (non-capitalised term) as used in this document may refer to: • An individual's digital identity – that is, an electronic representation of an individual or entity which enables that entity to be sufficiently distinguished when interacting online (refer Section 2.2) • The generic concept of digital identity; and/or • General/existing digital identity systems, activities and services (not specific to the Australian Government Digital Identity System). *Not to be confused with other usages in this document – i.e. "Digital Identity System" (see below), or the proposed legislative definition of "digital identity" (described in Section 5.3).
Digital Identity Program (the Program)	The Program being delivered by the DTA, in partnership with other government entities, which will, over time, allow individuals and government services to get more done online at any time and place they choose. The Program will give Australian citizens and permanent residents a single and secure way to create a Digital Identity that can be used to access online government services.
Digital Identity System (the System)	Generally, a digital identity system is a group of participants that work together to ensure identity-related information can be relied on by services/relying parties to make risk-based decisions. When capitalised in this document, refers specifically to the Australian Government Digital Identity System, as being delivered by the Program and proposed to be regulated through the Exposure Draft Bill and rules, as distinct from other digital identity systems.
Digital Transformation Agency (DTA)	The DTA is an agency of the Australian Government tasked with improving the accessibility and availability of government services online by helping government 'transform services to be simple, clear and fast'.

Digital Transformation Strategy (DTS)	The Digital Transformation Strategy sets the direction for the DTA's direction for work from 2018 - 2025. The accompanying Roadmap describes a rolling two-year window of work that has been planned.
Essential Eight	The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies to help technical cyber security professionals in all organisations mitigate cyber security incidents caused by various threats. The Essential Eight is a series of baseline mitigation strategies taken from the Strategies to Mitigate Cyber Security Incidents recommended for organisations. Implementing these strategies as a minimum makes it much harder for adversaries to compromise Systems.
Financial System Inquiry Report (Murray report)	The Financial System Inquiry Report (Murray report) was released on Sunday 7 December 2014. This report responded to the objective in the Inquiry's Terms of Reference to best position Australia's financial System to meet Australia's evolving needs and support economic growth. It offered a blueprint for an efficient and resilient financial System over the next 10 to 20 years characterised by the fair treatment of individuals. The Inquiry made 44 recommendations relating to the Australian financial System. These recommendations reflect the Inquiry's judgment and are based on evidence received by the Inquiry.
Government Business Enterprises (GBE)	A Government Business Enterprise (GBE) is an Australian Government entity or Australian Government company that is prescribed by the rules (section 8 of the PGPA Act). Section 5 of the PGPA Rule prescribes nine GBEs: two corporate Australian Government entities, and seven Australian Government companies.
Identity proofing (IP) levels	Different levels of identity strength defined by the TDIF, which can be used for differing purposes and when different levels of identity confidence are needed. These range from Level 1 (when no or a very low level of confidence is needed; supports self-assured identity), up to Level 4 (when a very high level of confidence is needed; requires in-person attendance of person claiming identity as well as three or more identity documents and biometric verification).
Information Security Manual (ISM)	The Australian Signals Directorate (ASD) produces the Australian Government Information Security Manual (ISM). The manual is the standard which governs the security of government ICT Systems. The manual comprises three documents targeting different levels which are: Executive Companion, Principles and Controls.
Information Security Registered Assessors Program (IRAP)	The Australian Signals Directorate (ASD) supports higher standards of cyber security assessment and training through the enhanced Information Security Registered Assessor Program (IRAP). IRAP endorses individuals from the private and public sectors to provide cyber security assessment services to Australian Governments. Endorsed IRAP assessors assist in securing ICT networks by independently assessing security compliance, suggesting mitigations and highlighting residual risks.
Interim Oversight Authority	The Interim Oversight Authority is the body under the DTA currently regulating the System, with support from Services Australia.

JobSeeker; JobKeeper	An income support payment set up in response to the economic impacts of the COVID-19 pandemic, the JobSeeker payment supports those between 22 and Age Pension age and looking for work. As part of its COVID-19 economic response, the Australian Taxation Office paid JobKeeper payments to employers. Eligible employers then paid JobKeeper payments to employees as part of their usual wages.
Know Your Customer (KYC) Obligations	The Know Your Customer (KYC) guidelines in financial services requires that professionals make an effort to verify the identity, suitability and risks involved with maintaining a business relationship. The producers fit within the broader scope of a bank's Anti-Money Laundering (AML) policy.
Memoranda of Understanding (MoU)	Unless otherwise indicated, refers to agreements or arrangements put in place between government entities, such as the System Governance Interim MoU between Services Australia and the DTA.
New Payments Platform (NPP)	Launched in February 2018, the New Payments Platform (NPP) is open access infrastructure for fast payments in Australia. The NPP was developed via industry collaboration to enable households, businesses and government entities to make simply addressed payments, with near real-time funds availability to the recipient, on a 24.7 basis.
Notifiable Data Breach Scheme (NDB Scheme)	The Notifiable Data Breaches (NDB) Scheme was established in February 2018 to improve consumer protection and drive better security standards for protecting personal information. It applies to entities and organisations who are covered by the Privacy Act and are required to take reasonable steps to secure personal information.
Office of the Australian Information Commissioner (OAIC)	The Office of the Australian Information Commissioner (OAIC) is an independent Australian Government agency, acting as the national data protection authority for Australia, established by the Australian Information Commissioner Act 2010 headed by the Australian Information Commissioner.
Organisation for Economic Co-operation Development (OECD)	The Organisation for Economic Co-operation and Development (OECD) produces independent analysis and statistics to promote policies to improve economic and social wellbeing across the globe.
Operating Rules	The Operating Rules set out the legal framework for the operation of the identity federation, including key rights, obligations and liabilities of participants.
Oversight Authority	The entity responsible for the administration and oversight of the identity federation in accordance with the Operating Rules and TDIF.
***Privacy Act 1988* (Cth) (Privacy Act)**	The *Privacy Act 1988* (Privacy Act) was introduced to promote and protect the privacy of individuals and to regulate how Australian Government entities and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information. The Privacy Act includes 13 Australian Privacy Principles (APPs), which apply to some private sector organisations, as well as most Australian Government entities.

Privacy Impact Assessment (PIA)	An assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.
Private Sector	The private sector is the part of the economy that is run by individuals and companies for profit and is not state controlled. For the purposes of this RIS, it encompasses all for-profit businesses that are not owned or operated by the government.
Protective Security Policy Framework (PSPF)	The Protective Security Policy Framework (PSPF) assists Australian Government entities to protect their people, information and assets, both at home and overseas. It sets out protective security policy and supports entities to effectively implement the policy across the following outcomes: security governance, information security, personnel security, physical security.
Regulatory Technology (RegTech)	Regulatory technology (RegTech) is the management of regulatory processes within the financial industry through technology. The main functions of RegTech include regulatory monitoring, reporting and compliance.
Trusted Digital Identity Framework (TDIF)	The TDIF contains the tools, rules and accreditation criteria to govern an identity federation. It provides the required structure and controls to deliver confidence to participants that all accredited providers in an identity federation have met their accreditation obligations and as such may be considered trustworthy.
World Economic Forum (WEF)	The World Economic Forum (WEF) is an international NGO founded on 24 January 1971. The WEF's mission is stated as “committed to improving the state of the world by engaging business, political, academic, and other leaders of society to shape global, regional, and industry agendas”.

Appendix B – Entities, interactions and incentives within the current System

The following table provides a more detailed description of the specific interactions and likely incentives of each type of entity currently involved in the System, as described and visually depicted in Section 2.3.3 Entities, interactions and incentives within the current System.

Entity type	Role, interactions and incentives within current System	Example participants
Onboarded accredited entity		
Identity provider (IDP)	Role: Provides the platform for verifying the identity of an individual online. IDPs undertake primary verification of an individual when a Digital Identity is established, and act as a conduit for the verification of additional information about individuals held by different participants. That is, providing a response to the query: 'Is this person Jane Doe?' Consistent with the 'choice' principle, the System was designed to include multiple IDPs, both government and non-government. If they choose to, people can switch to a different IDP while maintaining access to identity services. A non-Australian Government IDP (Australia Post's Digital iD) has been accredited but is not onboarded and available for individuals to select. Interactions: IDPs are the key contact point between the 'external' and 'internal' components of the System. They interact directly with people through the creation of Digital Identities, and seek consent from people each time a relying party seeks confirmation of their identity. They also interact directly with relying parties to receive and action requests for identity verification. Within the TDIF, IDPs then interact with an IDX to confirm an individual's identity details. The System is designed to ensure that IDPs do not have access to information about the services individuals' access. Incentives: The existing IDP is an Australian Government agency. It is incentivised to generate ongoing growth in uptake of Digital Identity because this will support expanded adoption and use of the System, justifying investment to date. At present there is no legislative mechanism by which IDPs can recover costs or charge other System participants for their services within the TDIF. While it is theoretically possible for non-government entities to become IDPs, in practice there are limited incentives to	myGovID Australia Post's Digital iD (accredited but not on-boarded and available in the System as an IDP choice)

Entity type	Role, interactions and incentives within current System	Example participants
	do so because only Australian Government agencies can currently become relying parties and there is no legislative mechanism for charging. This limits both the potential customer pool and the potential for revenue generation for identity services.	
Attribute service provider (AP)	Role: Supplies additional information about an individual to support verification of their identity and other attributes. APs provide authoritative information about entitlements, relationships or other characteristics – e.g. information on whether an individual is currently receiving a specific government payment or is authorised to act on behalf of a particular entity. That is, an AP can provide a positive or negative response to queries like: 'Is Jane Doe entitled to Family Tax Benefit?' or 'Is Jane Doe an authorised representative of Company A?' Interactions: An AP interacts directly only with the IDX. When a relying party requests verification of specific attributes about an individual via an IDP, this request is relayed to the IDX. The IDX then contacts the AP for confirmation of the attribute information being sought. Typically, an AP will be integrated with a registry that manages particular attributes. For example, the ATO's Relationship Authorisation Manager (RAM) system can verify relationships between an individual and a business. If a business wanted to authorise a particular individual to manage their taxes, this relationship could be verified by the RAM system acting as an AP. Incentives: Under the current System arrangements, APs are exclusively Australian Government agencies such as the ATO. These entities are resourced to participate in the System because their involvement supports the ongoing expansion of Digital Identity by diversifying the range of possible use cases.	ATO Relationship Authorisation Manager (RAM) MyGov (currently undergoing accreditation process – est. completion May '21)
Credential service provider (CSP)	Role: support the safety and security of the System. CSPs are accredited to undertake the functions of authentication credential management and take care of all credentials (i.e. passwords and other forms of access restrictions) used in the System. That is, a CSP can provide a positive or negative response to queries of the nature: 'Does this person's password match the password for the account held by Jane Doe?' or 'Does the biometric information provided match that previously provided by Jane Doe?' At present, the only accredited CSPs are also accredited as IDPs, providing an integrated solution for an individual to authenticate themselves when establishing a Digital Identity or authorising verification by a relying party.	myGovID Australia Post's Digital iD (accredited but not on-boarded and available in the System as a CSP choice)

Entity type	Role, interactions and incentives within current System	Example participants
	Interactions: CSPs interact with IDPs as part of the process for identity verification. Current CSPs are also IDPs, meaning this interaction occurs within a single system process. Incentives: Credentials management is an essential component of effective functioning of identity services. For this reason, there is a strong incentive for IDPs to also become accredited as CSPs. It is theoretically possible for an entity which is not an IDP to establish itself as a CSP, for example by providing specialised and high-security biometric credentials management. However, there are limited incentives to do so in the current system given the relying parties are exclusively Australian Government entities.	
Identity exchange (IDX)	Role: provides the infrastructure for interactions between other System participants to occur in a way that is secure and respects the privacy of individuals. With individual consent, IDX functions like a switchboard, transferring information between relying parties, IDPs and APs. That is, the IDX is the conduit by which answers to all queries addressed by the previous three participants are communicated. The IDX only passes on the specific information that an individual has authorised to be provided. Interactions: The IDX is the centrepiece of the System, managing interactions between all onboarded accredited entities operating within the TDIF. Incentives: The IDX is a crucial System role currently fulfilled by the Australian Government. The primary incentive for the IDX is to ensure efficient and secure transferral of information to support effective functioning of the overall System.	Services Australia
Relying parties		
Government relying parties	Role: rely on verified identity information, attributes or assertions provided by IDPs, Aps and CSP through the IDX to enable the provision of a digital service. That is, relying parties are the entities that *make* System queries such as 'Is this person Jane Doe?', 'Is Jane Doe entitled to Family Tax Benefit?' and 'Does this person's password match the password for the account held by Jane Doe?'. Relying parties can be considered one of two 'end users' for Digital Identity, along with individuals. Participation in the System is fully voluntary for relying parties. Interactions: Relying parties interact exclusively with IDXs. Incentives: Under current System arrangements, only government entities can legally become relying parties.	Various, including: Centrelink ATO State and territory revenue agencies (currently being tested under pilot conditions)

Entity type	Role, interactions and incentives within current System	Example participants
	Entities have a strong incentive to do so because the use of Digital Identity can significantly reduce the need for face-to-face or paper-based identity verification by citizens, delivering benefits such as: Reduced processing times for transactions requiring identity verification Improved customer experience by removing the need to visit a shopfront or provide certified copies of documents Reduced manual handling of paperwork and ability to re-direct associated resources to alternative tasks.	
Governance body	Role: responsible for the administration and oversight of the System, including ensuring the requirements of the TDIF are met by all onboarded accredited entities. The Interim Oversight Authority's functions are currently shared by the DTA and Services Australia. Interactions: The Interim Oversight Authority acts as the TDIF accreditation body, accrediting entities to act as IDPs, Aps and CSPs within the System. It then provides ongoing oversight of how entities behave within the System, ensuring compliance with the TDIF. In these roles, it interacts closely with all onboarded accredited entities. The Interim Oversight Authority may also interact with relying parties and Individuals in some limited cases where it receives complaints about onboarded accredited entity conduct. The Oversight Authority's role as System regulator means that nature of these interactions is different from that between other System participants. Specifically, it does not play a role in the day-to-day delivery of the System, instead having a higher-level oversight and governance role. Incentives: The Interim Oversight Authority is a Commonwealth government entity. Its primary incentives are to promote the efficient, safe and transparent operation of the System.	DTA and Services Australia
User	Role: establish and use a Digital Identity – through one or more providers – to verify their identity when accessing a range of digital services. That is, people are the *subject* of queries such as 'Is this person Jane Doe?', 'Is Jane Doe entitled to Family Tax Benefit?' and 'Does this person's password match the password for the account held by Jane Doe?'. Participation in the System is fully voluntary for individuals using either in their business (e.g. applying for an ABN) or personal capacity. Interactions: As the other 'end user' of digital identity (along with relying parties) individuals interact exclusively with IDPs. They establish a Digital Identity presence with an IDP	Individual citizens in private capacity Individuals in capacity as business owners

Entity type	Role, interactions and incentives within current System	Example participants
	and provide consent through it for the verification of their identity on each occasion this is sought by a relying party. While the range of interactions detailed above take place on behalf of individuals, this does not require direct contact between these people and any entity other than their chosen IDP. It should be noted that people are likely to interact directly with onboarded accredited entities through other channels – e.g. lodging tax returns with the ATO or applying for benefits through Services Australia. These interactions form the basis for Participants holding individuals' information which can subsequently be used to verify their identity /attributes. However, these interactions occur outside the System and would do so if it were not in place. Incentives: Users have a range of incentives to participate in the System, including: • Improved convenience and speed of processing when interacting with Australian Government agencies • Strengthened autonomy and control over which entities will hold information on their identity and attributes • Reduced risk of identity theft due to strong levels of security built into the System. However, it should be noted that there are several factors that may also incentivise *against* individual participation, including: • concern over government centralisation or control of information on their identity and attributes • lack of a robust legal framework for protecting privacy, and ensuring compliance with the TDIF • limited useability of digital identity outside of interaction with Australian Government entities.	

Table 9: Details of entities, interactions and incentives within the current System

Appendix C – Entities, interactions and incentives within an expanded System

The following table provides a more detailed description of the specific interactions and likely incentives of each type of entity that would be able to participate in an expanded System, as described and visually depicted in Section 2.5.2 Entities, interactions and incentives within an expanded System.

Entity type	Potential role, interactions and incentives in an expanded System	Example participants
Onboarded accredited entities		
Identity provider (IDP)	Role: As in 'Current' table above. Under an expanded System it is anticipated that private sector entities would be more likely to seek to participate as IDPs, due to the below incentives. Interactions: As in 'Current' table above. Regardless of which entities choose to become IDPs, the nature of their interactions with other components of the System will remain the same. This is intended to ensure competitive neutrality between government IDPs and other System participants. Incentives: An expanded system will pave the way for a significantly larger number of organisations and individuals to participate in the System, as relying parties and individuals. This is because non-government entities will be able to become relying parties for the first time, thereby expanding the range of Digital Identity use cases for individuals. Under this expansion, there are expected to be significantly stronger incentives for new, non-government IDPs to enter the market and compete with existing government/quasi-government IDPs. An increased number of relying parties creates a larger potential customer pool for IDPs, beyond government entities. As more entities seek to become relying parties, this also increases the range of services and contexts in which individuals can use Digital Identity, creating a self-reinforcing loop of more relying parties generating more individual participants, and more individuals supporting increased uptake by relying parties. Private sector IDPs will face different financial incentives than existing IDPs. It is anticipated that these entities will only participate in the System where there is an opportunity for them to gain financially from doing so. The Australian Government has acknowledged this and	In addition to current: Private sector (e.g. financial services institutions, identity management agencies)

Entity type	Potential role, interactions and incentives in an expanded System	Example participants
	initiated design work on an appropriate charging regime for the System as part of its expansion planning. Within the bounds of this framework, private sector IDPs would be expected to seek to recover the costs of participation through fee-for-service arrangements. Service efficiency principles suggest it would be easier to recover these costs through relying parties on a contract basis than from people on an individual transaction basis. Any steps by the Commonwealth to regulate IDP behaviour through the charging regime would also affect the specific incentives for IDPs. As participation is entirely voluntary, private sector IDPs would only be expected to participate in an expanded System where charging arrangements do not impose unreasonably high costs, or where such costs can be recouped through other System participants (e.g. relying parties) at a level and in a manner which does not inhibit uptake by those participants.	
Attribute service provider (AP)	Role: As in 'Current' table above. There are a wide range of entities outside of the Australian Government holding information on individuals' attributes. For example, a relying party may need to verify whether a particular individual holds a specific university qualification, or is a member of a compulsory professional body. Under an expanded System, a wider range of these entities would be able to participate as APs. This would result in both efficiency benefits and revenue opportunities for participating entities. Interactions: As in 'Current' table above. Regardless of which entities choose to become APs, the nature of their interactions with other components of the System will remain the same. Incentives: As with IDPs, under an expanded System it would be possible for APs to generate revenue through the provision of attribute verification services. For example, an AP may charge an IDP a small fee for each attribute verified, with this fee then being reflected in the aggregate fee a relying party is charged for the IDP's services. APs and IDPs are likely to be incentivised to enter into volume-based arrangements within such a charging framework. It should also be noted that the expansion of the System has the potential to lead to significant efficiencies for entities which are enabled to become APs. For example, professional bodies may already handle a volume of requests to confirm an individual's accreditation outside of the System. Where entities already deal with such	In addition to existing Australian Government entities: State, territory and local governments Universities Professional bodies Credit ratings agencies

Entity type	Potential role, interactions and incentives in an expanded System	Example participants
	requests by manual /paper-based means, considerable efficiencies may be achieved by becoming an AP and processing requests within the System instead.	
Credential service provider (CSP)	Role: As in 'Current' table above. Interactions: As in 'Current' table above. However, the expansion of the System creates the opportunity for entities to participate as standalone CSPs, rather than this function being combined with that of an IDP. Incentives: The expansion of the System would potentially create incentives for new entities to participate as standalone CSPs where they are able to provide bespoke or niche credentialing services. For example, private security companies may seek to provide highly-secure credentialing services based on advanced biometrics, for use by private sector IDPs and relying parties which need very high levels of reliability in identity verification. As with private sector IDPs, entities are only expected to participate in the system as standalone CSPs where there is a market opportunity to do so, given such participation is voluntary.	In addition to existing Australian Government CSPs: Private sector IDPs Private sector security solution providers
Identity exchange (IDX)	Role: As in 'Current' table above. Whilst there is no legal barrier to a non-government IDX, it is not anticipated that this function would be transferred to entities beyond the Australian Government in the medium term. Interactions: As above. Incentives: As above.	Anticipated the Commonwealth government will remain the sole provider of the IDX for the foreseeable future.
Relying parties		
Non-Commonwealth relying party	Role: As in 'Current' table above. A key feature of an expanded System is the capacity for entities beyond the Australian Government to become relying parties. However, participation in the System as a relying party would remain entirely voluntary. Interactions: As in 'Current' table above. Under an expanded System, relying parties would likely have a greater choice of IDPs to transact with, due to the entry of private sector IDPs in competition with myGovID. Incentives: As with government relying parties, other government and private sector entities would be expected to experience the following benefits from participation in the System: • Improved processing times for transactions requiring identity verification • Improved customer experience by removing the need for people to attend venues in person or provide physical documents	In addition to Australian Government entities: State, territory and local government entities Financial services providers Utilities and telecommunications providers Recruitment agencies

Entity type	Potential role, interactions and incentives in an expanded System	Example participants
	• Reduced manual handling of paperwork and ability to re-direct associated resources to alternative tasks. These are likely to incentivise strong uptake by non-government relying parties under an expanded System. In this instance, non-government relying parties would be expected to seek the most cost-efficient commercial arrangements possible with IDPs for the provision of identity verification services. Increased competition through the entry of more IDPs to the System would be expected to put downward pressure on pricing for such services. These relying parties may also seek to undertake cost recovery through the pricing of services provided to Users. Their capacity to do so directly would be determined by any specific provisions within the charging regime when determined. However, this would not necessarily prohibit indirect cost recovery – for example through charging higher overall prices for services. Under an expanded System, it is anticipated that participation by private sector relying parties will be influenced to a greater degree by these financial and commercial considerations than is currently the case for government relying parties.	
Permanent governance body	Role: As in 'Current' table above. The permanent governance body for an expanded System could be a legislated function of a new or existing government agency. Interactions: Similar interactions as above, continuing to oversee the accreditation process and operating rules governing how these entities act within the System. However, unlike the status quo, it would be expected that a governance body within an expanded System may have increased interaction with relying parties, particularly relating to any new charging framework applying to the System which would impact relying parties (but not Users). Incentives: As an Australian Government entity, the permanent governance body's primary incentive would remain promoting the efficient, safe and transparent operation of the expanded System. It may have other stated objectives set out in any establishing legislation, for example accountability and independence.	A new or existing government agency given regulatory functions in relation to the System
User	Role: As in 'Current' table above. The role of users is expected to remain constant regardless of which IDPs	Individual citizens in private capacity

Entity type	Potential role, interactions and incentives in an expanded System	Example participants
	they choose to use. Participation in the System would remain fully voluntary. Interactions: Under an expanded System, users would be expected to have a wider range of IDPs to choose from because of the incentives discussed above for the entities. Users would also be able to access Digital Identity to verify themselves with a much wider range of relying parties, as non-government entities are enabled to join the System for the first time. Incentives: An expanded System offers increased incentives for participation by users, including: • improved convenience and speed of processing when interacting with a wide range of government and private sector entities • strengthened autonomy and control over which entities will hold information on their identity and attributes • reduced risk of identity theft due to strong levels of security built into the System. An expanded System also addresses several of the potential disincentives for users discussed in 'Current' table above, further strengthening the incentive to participate: • Reduced concern over government centralisation or control of information on their identity and attributes because of increased choice of IDPs • Strengthened legal framework for protecting user privacy, and ensuring the requirements of the TDIF are met • Strengthened useability of digital identity outside of interaction with government entities. As direct charging of users is not anticipated within an expanded System, these participants would not generally be incentivised to 'shop around' between IDPs. However, there is likely to be a positive feedback loop between the range of services (relying parties) a user can access with their chosen IDP and ongoing uptake of that IDP's services. These indirect competitive dynamics can be observed in other digital service delivery contexts, such as food delivery and ride-sharing apps.	Individuals in capacity as business owners

Table 10: Details of potential entities, interactions and incentives in an expanded System

Appendix D – Previous consultations

The following table details the Program's history of previous consultations relevant to the regulation of Digital Identity. Consultation is ongoing, however the list below is correct as at September 2021.

Consultation	Details	Timeframe occurred	No. of stakeholders engaged
Privacy Impact Assessments (PIA)	There have been multiple PIAs conducted on Digital Identity, all of which have involved engagement with a variety of stakeholders on privacy, consumer protection and security issues.	Initial PIA for the TDIF Alpha - December 2016 through to present	Refer to Strengthening privacy under the TDIF | Digital Transformation Agency (dta.gov.au) for full copies and details of stakeholder engagement.
TDIF public consultations	There have been four releases of public consultation on the TDIF to date. These consultations are designed to elicit stakeholder views on all elements of the TDIF to ensure a consistent approach is taken to usability, accessibility, privacy protection, security and more.	Four TDIF releases – respectively February 2018, August 2018, April 2019 and May 2020 - (next scheduled review will occur by July 2022)	Broad consultations with government, privacy experts and industry associations. More than 2450 comments received over 3 rounds of consultation.
Targeted consultation with Australian Government agencies	Relevant Australian Government agencies were consulted for their input on an initial Scoping Paper and a draft Consultation Paper prior to their respective public releases. This occurred through the Digital Identity Legislation Working Group (DILWG), a forum with representation from thirteen Australian Government agencies.	Scoping Paper phase - March 2020 Draft Consultation phase - August 2020.	Scoping Paper phase - 23 Australian Government agencies Draft Consultation phase - 17 Australian Government agencies
Targeted consultation with states and territories	States and territories were initially engaged for commentary at the early stages of policy development. This consultation occurred through the Digital Identity Cross Jurisdictional Working Group (DICJWG), a forum with representation from all eight states and territories in	Throughout 2020	8 states and territories in Australia Themed workshop invitations sent to all Australian jurisdictions

Consultation	Details	Timeframe occurred	No. of stakeholders engaged
	Australia. The DICJWG conducted four themed workshops inviting engagement in formulation of the three policy options.		
Targeted consultation with financial institutions	The Program met with twelve key financial institutions across 2020, some numerous times, to discuss issues related to potential regulation.	Throughout 2020	12 financial institutions
Public consultation paper	The public consultation paper on legislation sought government, community, industry and individual views on the scope, nature and extent of possible government regulation of the System. Supporting the release of the paper was five webinars, aimed at academics, advocacy groups, private sector, state and territory privacy commissioners and the public. A consultation synthesis report was subsequently published online, and summarised key messages, themes and outcomes of the public consultation paper process. Finally, a position paper was released online for further public consultation and provided updated assessments of key policy positions and the nature of potential regulation.	Public Consultation Paper – November to December 2020 Consultation Synthesis Report – published 12 February 2021 Position Paper – published 10 June 2021	Supporting webinars - attended by 110 stakeholders Public consultation paper - received 44 submissions (16 state and territory government, 20 private sector, 8 individuals and consumer groups) Position paper – received 62 submissions
Targeted consultations with critical stakeholders	Further targeted consultation occurred across key areas from the synthesis report, in the form of one-on-one engagements, Q&A sessions and webinars. Stakeholders engaged include the Privacy Information Commissioner's group, state and territory governments, the Australian Government Digital Identity Working Group, private	Early months of 2021	23 submissions received

Consultation	Details	Timeframe occurred	No. of stakeholders engaged
	sector groups, non-for-profit sector groups and various programs/status groups. Feedback was incorporated into the position paper.		
Targeted events with key industry and government associations	Following release of the position paper, targeted events with key industry and government associations occurred, in order to facilitate open conversation and consideration of broad-ranging perspectives prior to the release of the Exposure Draft package. Targeted events included roundtables and Q&A sessions.	Roundtables: • Australian Institute of International Affairs (AIIA) – 1 July 2021 • Australian Society for Computers and the Law (AUSCL) – 13 July 2021 Q&A sessions: • Banking sector – July 2021 • Government sector – July 2021	Roundtables: • AIIA – attended by over 50 stakeholders • AUSCL – attended by around 70 stakeholders Q&A sessions: • Banking sector – attended by around 6 stakeholders • Government sector – attended by around 15 stakeholders

Table 11: Program's previous and relevant consultations held to date

Appendix E – Regulatory costs: Methodology and assumptions

This Appendix summarises the approach to estimating regulatory costs in this version of the RIS. These estimates are not definitive nor final but are provided as "placeholders" for consideration and validation by entities. The costs are presented in this RIS on a per-entity basis, however the final version of the RIS will combine consultation data with other sources to develop economy-wide, annualised regulatory burden estimates for each option in accordance with the Regulatory Burden Measurement Framework.

Methodology

Per-entity regulatory cost estimates included in this document have been developed in accordance with the below approach:

1. Identifying the activities that would influence regulatory costs of a regulated entity under the relevant option (for example, the Regulatory Impact Tables at Section 9.2 Regulatory Impacts) as either onboarding, compliance, ongoing or administration.
2. Categorising the activity as either initial (i.e. a mobilisation or initial cost incurring in Initial Year only), ad hoc (occurring less predictably and frequently more than once) or ongoing (if occurrence is known and frequent more than once, e.g. ongoing maintenance / monitoring obligations).
3. For post-Initial Year ad hoc activities, making assumptions on the expected annual frequency of each activity. These assumptions were informed by Government's experience working with the System to date and internally tested but will be refined on an ongoing basis.
4. Estimating the resource effort (time taken) to comply with that requirement (including low-range and high-range for each activity).
5. Estimating the labour costs associated with a regulatory task, by multiplying the time taken to complete the required compliance activity (low and high range) by the expected annual frequency of each activity and by the hourly cost for the relevant staff.

6. This provides the cost of complying with the regulatory requirement for each option and entity group as relevant, and is the basis for the per-entity regulatory cost ranges in the RIS.

Note – the above approach was followed for all entity groups for Option 3. As Option 2 involves a smaller proportion of regulatory measures compared to Option 3 (mainly privacy-related), this was costed (for GBEs) by focusing on the privacy sub-set of activities in the tables on Section 9.2 Regulatory Impacts. Option 2 does not distinguish between Year 1 and Post-Year 1 costs, because there are limited "initial" regulatory requirements involved.

Assumptions and sources

The key assumptions and sources used for regulatory cost estimates are described below:

- **Initial Year and post-Initial Year activity classifications** – these classifications were derived from analysis of the nature of the regulatory activities prescribed per individual regulated entity for each considered option. Initial Year activities were assumed to occur once in the first year of option adoption, and generally included onboarding or initial accreditation activities. Other ad-hoc or ongoing compliance activities undertaken during the Initial Year were estimated based on the assumed frequency of undertaking the activities. The frequency of Post-Initial Year ongoing activities were considered based upon the nature of the activity (e.g. whether an ongoing monitoring / maintenance obligation, or a one-off activity that may be needed throughout the year). These assumptions have been internally tested and will also be tested through this public consultation process.
- **Labour rates** – In accordance with Australian Government guidance, the default hourly labour rate contained within the Regulatory Burden Measurement Framework has been used. This is based on average weekly earnings, but adjusted to include income tax. This provides an economy-wide value for employees of $41.74 per hour. This value is then scaled up using a multiplier of 1.75 (or 75 per cent as it is input into the Regulatory Burden Measure) to account for the non-wage labour on-costs (for example, payroll tax and superannuation) and overhead costs (for example, rent, telephone, electricity

and information technology equipment expenses). This results in a scaled-up rate of $73.05 per hour ($41.74 multiplied by 1.75). Australian Government guidance is that this default rate should be used in cases where regulation cuts across a number of sectors, as is the case for regulation of the System. Note – the rates in the Regulatory Burden Measurement Framework latest version (March 2020) were escalated to FY21/22 dollars using the Australian Bureau of Statistics' Wage Price Index (WPI) average indexation of 1.5 % per year.

- **Resource efforts** – were estimated based off analysis of the regulatory activities prescribed per individual regulated entity for each considered option. This analysis was informed by Government's current understanding of the potential future regulatory activities, as detailed in the Exposure Draft package (and where activities were considered within the scope of the Regulatory Burden Measurement Framework). Indicative resource effort ranges were provided to accommodate for potential uncertainty around estimated numbers. It is expected that the submissions to this Consultation RIS will provide more accurate data around the resource efforts required by affected non-government entities.
- **Contingency costs** – Contingency is included as an approximate allocation within the resource hours (low to high).
- **General** – It has been determined that this RIS will over-estimate, rather than under-estimate, the potential regulatory costs. This has been a guiding principle through this costing, including in making assumptions. For example, for the purposes of costing it has been assumed that all entities will seek to receive restricted attributes (and be subject to the corresponding regulatory requirements), whereas this is not expected to be the case once regulation is in place.

Appendix F - Figures and tables

A.1 Figures

A.2 Tables