Australia's Digital ID System

Australian Government

Impact Analysis: Legislating the Australian Government Digital ID Program

www.digitalidentity.gov.au

Department of Finance

Version: 1801

Contents

1 Executive summary

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

The Australian Government Digital ID System (AGDIS) is a federated model where accredited entities establish and authenticate Digital IDs for people in a trusted environment. The AGDIS is currently used by over 11 million people and over 1.5 million businesses to access more than 135 digital government services. Expansion of the AGDIS and establishment of the permanent Accreditation Scheme will enable state and territory governments and private sector involvement.

The Government's vision for the AGDIS is a national, economy-wide system that provides Australians with a voluntary, secure, convenient and inclusive way of verifying who they are when interacting with government and businesses online. People will be able to verify their identity with their choice of identity providers to create a Digital ID. They will be able to simply, safely and securely reuse their chosen Digital ID 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 ID across Australia. This means the future AGDIS will have domestic interoperability across states and territories.

Having delivered the foundational capability and infrastructure, governing policy, security and risk management frameworks, and underlying operational support, Digital ID is now looking to expand in several phases. This expansion will first focus on making the AGDIS available to more Commonwealth and state entities, before becoming integrating further with state and territory government Digital ID services, then finally private sector services. The end state of Digital ID being available as a 'whole-of-economy solution' would enable all individuals and businesses to have

more secure and convenient engagement with government (including state, territory and local) services and the private sector.

1.3 The need for Government intervention

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 ID's benefits, particularly as it expands across the Australian economy. These are:

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

Regulatory action is required to address the above barriers to uptake of individuals and market entry by firms, enabling non-Government participation; and legislatively entrenching privacy, security and permanent governance arrangements to enhance confidence and trust in the AGDIS and the Accreditation Scheme. Three options have been considered to address these gaps:

- retaining the status quo (i.e. no regulatory action taken)
- leveraging existing regulatory schemes (primarily addressing privacy-related issues)
- establishing a dedicated Digital ID regulatory scheme through legislation and nominating the Australian Competition and Consumer Commission (ACCC) as the initial regulator.

In recent years, the potential and growing demand for the AGDIS has been clearly demonstrated, with large scale events effecting a number of Australians in some capacity such as the private sector cyber security breaches of Optus, Medibank Private and Latitude Financial (the recent cyber breaches). The Black Summer bushfires of 2019-20 and COVID-19 pandemic both saw an unprecedented increase

in the use of digital channels to access stimulus measures, closely followed by floods in early 2022.

This Impact Analysis has been developed to examine the case for establishing a dedicated regulatory scheme for the AGDIS and the likely impacts (regulatory and non-regulatory) of proposed measures. It describes the problem that Government is trying to solve and proposes options. These have been informed by wide stakeholder consultation to validate expected impacts. The Impact Analysis recommends that Government implement the option with the highest net benefit – a dedicated regulatory scheme established through legislation. Each of the seven Impact Analysis questions, and the applicable section(s) that address them, are set out in Table 1.

Impact Analysis question	Relevant document section
1 What is the policy problem you are trying to solve and what data are available?	3 What is the problem?
2 Why is government action needed, and how will success be measured?	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
6 What is the best option from those you have considered and how will it be implemented?	11 Best option from those considered
7 How will you implement and evaluate your chosen option?	12 Implementation and evaluation of selected option

Table 1: Impact Analysis questions and relevant document section(s)

Benefits to the owners of a Digital ID in these events include the ability to identify themselves immediately and help provide rapid access to government support. In regard to the recent cyber breaches one of the underlying challenges has been the

amount of personal information held by organisations. Digital IDs present a clear benefit in that they limit the need for organisations to collect and store personal information. Research on the whole-of-economy value of Digital ID and the specific scope and parameters of this analysis, is discussed further at Section 2.5. The case for expanding the AGDIS.

Expanding Digital ID to state, territory and local governments presents efficiency opportunities across the multiple touchpoints between individuals and governments (for example in driver licensing authorities; using information from registers of births, deaths and marriages; healthcare; education; and utilities). However, even without this expansion, the AGDIS is a viable way to deliver Australian Government digital services more efficiently.

Another cornerstone of the proposed reforms is to establish an Accreditation Scheme that strengthens the existing accreditation framework for Digital ID service providers. The Accreditation Scheme will be underpinned by rigorous technical standards and robust enforcement mechanisms. Accreditation demonstrates that Digital ID providers meet high standards in areas such as privacy, cyber security and user experience.

1.2 The Net Benefits of Digital ID

The Department of Finance (Finance), in collaboration with other government entities, is leading the development of the whole-of-economy Digital ID System, also known as the AGDIS and the Accreditation Scheme. This Regulation Impact Statement (Impact Analysis) finds that the preferred option for Australia's Digital ID System combines reform of the AGDIS, alongside the establishment of a voluntary accreditation system for non-Government ID providers, as it has the highest net benefit. This includes additional regulatory costs for newly regulated entities, estimated to total around $1.5 million per year. However, these costs will be offset by select indirect benefits across the whole of economy, estimated to be around $3 billion per year. These impacts have been consulted on and are discussed in this document.

2 Introduction

2.1 Purpose of this document

This document examines the case for regulating the AGDIS, 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 recommended option (Option 3: Dedicated legislation to establish new regulatory scheme).

Consistent with Australian Government guidance, the Impact Analysis has been developed iteratively alongside the policy development process. An earlier version was released publicly for consultation in October 2021 to test and validate the impacts of options on stakeholders, with feedback received used to inform the most recent Draft Bill. Additional public consultation as well as a submission and survey process commenced in September 2023, and have informed advice to the Minister on the development of legislation.

2.2 What is a Digital ID?

A Digital ID is a safe, secure and convenient way for Australians to prove who they are online. The user will create a Digital ID by using existing issued government identity documents which are verified online with the issuing source (for example - verifying a driver licence with the issuing road authority and a birth certificate with the relevant Birth, Deaths and Marriages Registry). 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 ID 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 ID is not a single, universal or mandatory number, identifier 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 ID does not replace physical identification documents such as a birth certificate, visa or driver's licence and still remains voluntary in most cases. For Government services, there is an explicit

provision in the Bill (s71(1)) relating to the (AGDIS that requires an entity who is relying on a person's attributes (a "participating relying party") not to require an individual to create a Digital ID. This provision is designed to ensure that Digital ID does not change existing service requirements, and that it doesn't impede services being available to individuals. The choice to use a Digital ID to access these services will not replace existing options and is instead designed to add a secure and convenient channel, in addition to existing channels. This means existing alternate channels (such as telephone) need to be maintained as alternatives. There are two exceptions to voluntariness for an individual adopting a Digital ID, outlined in s71(3).

For non-Commonwealth Government services, there are no explicit voluntariness requirements in the legislation where services are operating outside of AGDIS. Voluntariness is intended to be achieved through competition and the ability for an individual to choose alternative service offerings.

There are multiple identity proofing levels offering different degrees of proofing rigour and identity confidence which can be used for differing purposes (and 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 ID, must consent to each transaction, and will be able to close their account at any time they wish.

2.3 Australian Government's Digital ID System (AGDIS)

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 (Murray inquiry) found that Australia's current identity environment is fragmented and uncoordinated. In the past, government entities have largely operated in silos, developing bespoke identity initiatives to manage internal fraud risks or to deliver specific policy outcomes. As described in the Murray inquiry, 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 inquiry recommended a national identity strategy that would improve efficiency and security across the digital economy.

Through the Digital ID Program, 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 Digital ID system – the AGDIS, 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 narrowing the difference between customer experience offered by government and the private sector.

To date, the Program has delivered the core foundations for the platform and is currently used by nearly half the population aged over 15 years (approximately 11 million people and over 1.5 million businesses) to access more than 135 digital government services.

2.3.2 Digital ID System governance: Trusted Digital Identity Framework (TDIF)

The TDIF, developed in collaboration with government entities, peak industry bodies, privacy commissioners and other stakeholders, is how the AGIDS 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 Digital ID System in Australia.

The TDIF is built around eight guiding principles: user centric, voluntary and transparent, service delivery focused, privacy enhancing, collaborative, interoperable, adaptable, and secure and resilient. These principles work to ensure that privacy and the security of personal information remain central to the Digital ID System. An individual may have multiple Digital IDs, 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 AGDIS remains secure and trustworthy. Entities are accredited as one or multiple roles specified within the TDIF (e.g. attribute provider or identity provider).

Accredited entities may choose one of three ways to participate in the Commonwealth's ecosystem:

- Achieve accreditation to be recognised as meeting the Commonwealth Government's high standards in providing identity services.
- Achieve accreditation to participate in the AGDIS. 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 that are accredited may or may not also be 'onboarded' to AGDIS, referring to establishing the physical technical connection of the entity's system to AGDIS. 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 AGDIS are described further 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 Digital ID. Does not need to be accredited nor onboarded
- **onboarded accredited (participating) entities** – entities that are accredited and onboarded to AGDIS. Roles which require accreditation are attribute provider (**AP**), credential service provider (**CSP**), identity exchange (**IDX**) and identity provider (**IDP**)
- **relying parties** (services) – a party that relies upon verified information provided through the AGDIS 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 AGDIS for several 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 role and prove this through annual assessments.

Interim Oversight Authority

The Interim Oversight Authority is responsible for the administration and oversight of the AGDIS. Its functions are shared by Finance 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 Digital ID System. Accordingly, the Interim Oversight Authority holds a broad range of powers established through the AGDIS Governance Agreement that enable it to carry out its governance and operational responsibilities. These include:

- applicant accreditation and annual assessment
- approval of participants and management of the participant register
- onboarding participants to the AGDIS
- monitoring participant compliance in accordance with the TDIF and operating rules
- inquiries, investigations and coordination (but not limited to) of AGDIS 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 AGDIS.

2.3.3 Entities, interactions and incentives within the current AGDIS

Figure 1 portrays the entities currently involved in the AGDIS and explains their interactions and likely incentives. A more detailed description of these for each type of entity is 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.

Onboarded 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 AGDIS. 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 Identity Exchange (**IDX)**, Attribute Service Provider (**AP)**, Credential Service Provider (**CSP)** and Identity Provider (**IDP).** There are also key entities within the AGDIS 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 ID. (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 AGDIS
- **users** – who create one or more digital identities and use these to access services via relying parties.

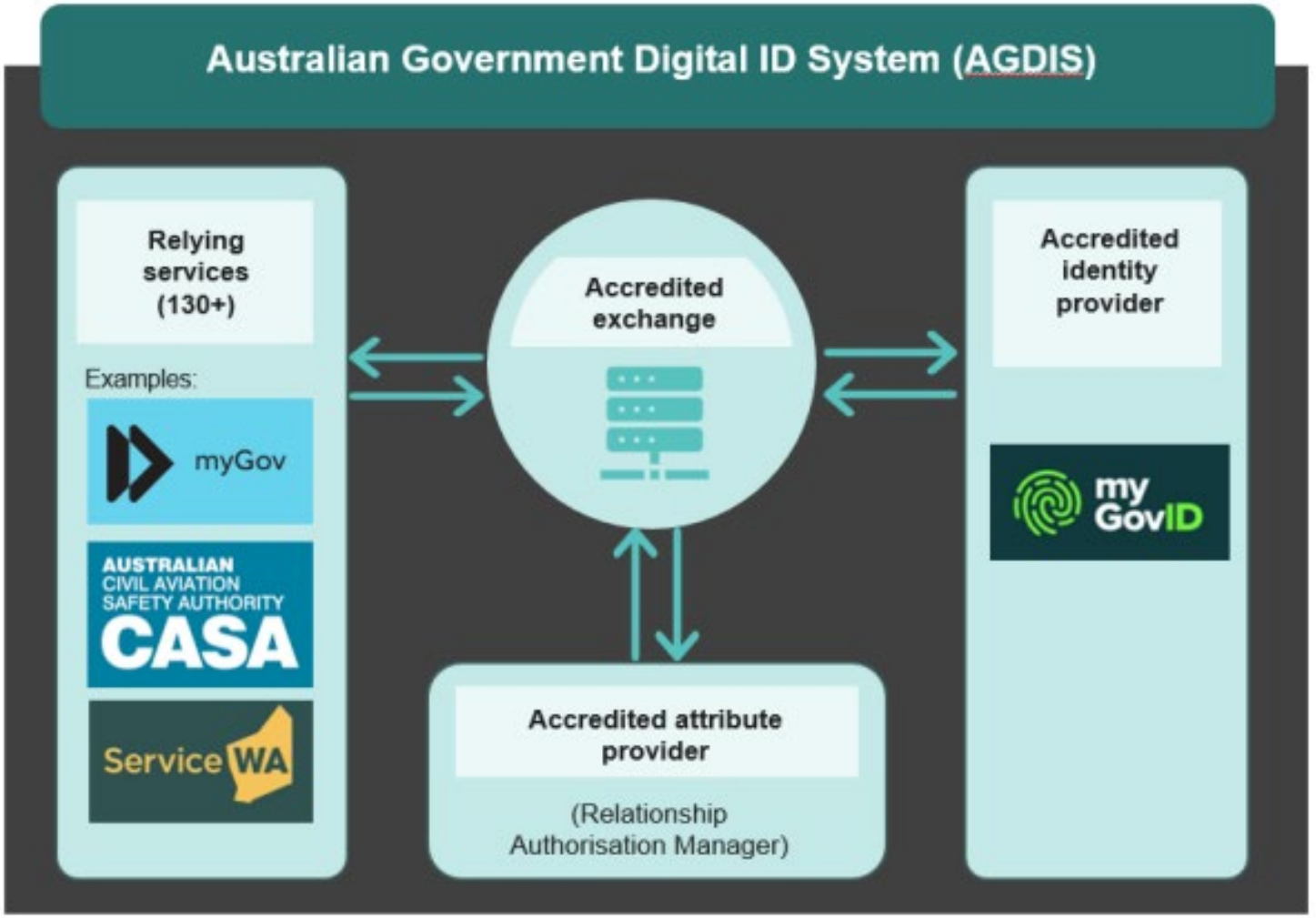


Figure 1: Entities, interactions and incentives within the current AGDIS

2.4 Benefits and value of Australia's Digital ID System for stakeholders

Digital ID offers the potential to assist individuals, businesses, government, and the overall economy in many different ways. The key benefits available from a whole-of-economy Digital ID system, which will also help to drive uptake, include:

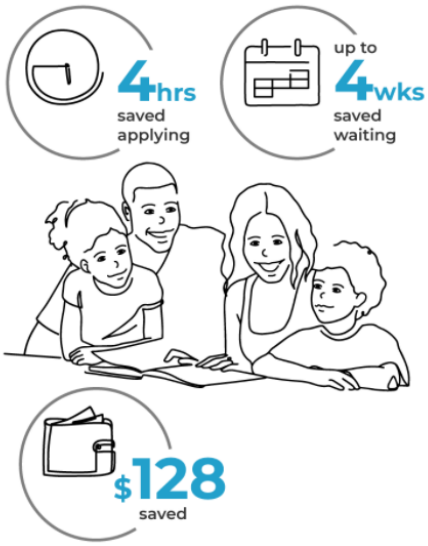
- For individuals (users):
  - reduced risk of information or data loss, data spill and identity fraud, encouraging greater confidence in Digital ID
  - improved speed of interaction with a wider range of Australian Government, state, territory and local government entities, as well as private sector businesses
  - greater choice and flexibility in interactions with identity providers, appealing to individuals' varying preferences
  - 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 benefits available to individuals and families are illustrated through the examples below.

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 ID 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 ID. With his Digital ID, he doesn't need to wait for replacement documents, and he can still access all the government services he needs.

Case study: Onboarding new employees

Jenny is an engineer who has recently secured a new job at a large Australian engineering company. Due to the number of sensitive and government projects they deliver, the company requires all new starters to complete a National Police Check (NPC).

Having completed an NPC previously, Jenny knows that this process requires her to provide 100 points of ID and can take up to 2 hours due to the number of steps including physically gathering, verifying, digitally scanning and uploading all relevant documentation.

Jenny already has a Digital ID account and finds that by consenting for her Identity Service Provider to share some information from her (already provided and verified) identity documents for the purposes of obtaining a NPC, the process takes significantly less time than it otherwise would have. Using the System saves her 1 hour 55 minutes and $69 in avoided costs.

Note - the benefits in this case study are available under an expanded System only.

- 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 regulatory 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 examples below.

Case study: Starting a new business

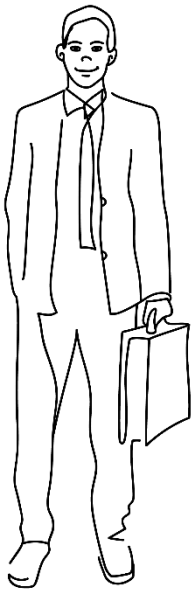
Alex is an IT specialist who decides to fulfill his long-term ambition of starting his own small business. He wants to get his new business off the ground as quickly as possible, particularly because he is the primary earner in his family.

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 ID. Alex finds the process takes a quarter of the time it otherwise would have, and he also saves $128 in avoided costs.

Case study: Applying for a business loan

Having started his new IT business, Alex is now seeking a loan to cover up-front costs, such as purchasing equipment and leasing office space.



Typically, there would be several steps for Alex to apply for the loan, including gathering identity and other documentation, completing information collection and application processes, and potentially visiting the bank in person.

Alex's bank offers the option of using his Digital ID to complete the information collection and application process. Alex finds the process takes significantly less time than it otherwise would have, saving him $140 in avoided costs. Alex is able to start operating his business sooner by spending less time applying for the loan and verifying his identity.

Note - the benefits in this case study are available under an expanded Digital ID system only.

- 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, which further reduces 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 AGDIS 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 ID
  - reduced costs to the economy, linked to reduced rates 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 AGDIS being that people, businesses and agencies choose to become a part of the AGDIS, a broad range of stakeholder expectations have been consistently considered to ensure AGDIS provides a service that benefits all that use it.

2.5 The case for expanding AGDIS

2.5.1 Benefits of expansion

The Australian Governments Digital ID 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. Rather than being a tactical solution designed to address the immediate issues faced as a result of COVID-19, AGDIS provides a more strategic and longer-term whole-of-economy solution.

While Digital ID'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. Australian Bureau of Statistics (ABS) data reinforces the expectation that increased demand for government services will continue, with small, medium and regional businesses, in particular, urgently needing a simple, safe and secure way to access critical services, payments and support to assist their ongoing recovery. Recent ABS statistics indicate there are 539,700 unemployed Australians as of August 2023, most of whom would be accessing some type of government support. However, in more extreme cases, This includes the ability to access services in times of increased need, more quickly, such as black swan events (COVID-19) that lead to people needing to access welfare services. The expansion of AGDIS 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 AGDIS can generate significant administrative efficiency, by enabling reduced paperwork, faster transactions and improved convenience. These benefits are expected to support state and territory government services, including the registration of births, deaths and marriages; licensing; utilities; healthcare; and education. These levels of government would also realise other benefits described above, including reduced identity fraud.

Digital ID is essential for the growth of the digital economy more broadly. It has a pivotal role to play in rebooting the global economy in the aftermath of the COVID-19 pandemic and beyond through digital and physical engagement with public and private sector services.

This assessment of the commercial opportunities available is supported by analysis commissioned in 2016 by the Digital Transformation Agency (DTA) (then the 'Digital Transformation Office') from Deloitte Access Economics, which found that System expansion presented expanded market opportunities across several integrated service offerings. These included in design, maintenance and operation of credentials and tokens, identity provision and disruptive emerging models for financial transactions and online communications, as well as for identity providers in general (for example, vendors may potentially sell other services to individuals as part of a verification 'one-stop shop'). The commercial appeal of these opportunities was recently validated with Australian payment network eftpos achieving the first private sector exchange accreditation under the TDIF in September 2021.

2.5.2 Entities, interactions and incentives within an expanded AGDIS

Figure 2 below depicts the entities that would be able to participate in an expanded AGDIS, 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 AGDIS , is the inclusion of non-Australian Government 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 remains broadly the same.

Non-Commonwealth agencies can currently participate in AGDIS 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 with an expanded scheme with a legislative charging framework. Under an expanded AGDIS 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.

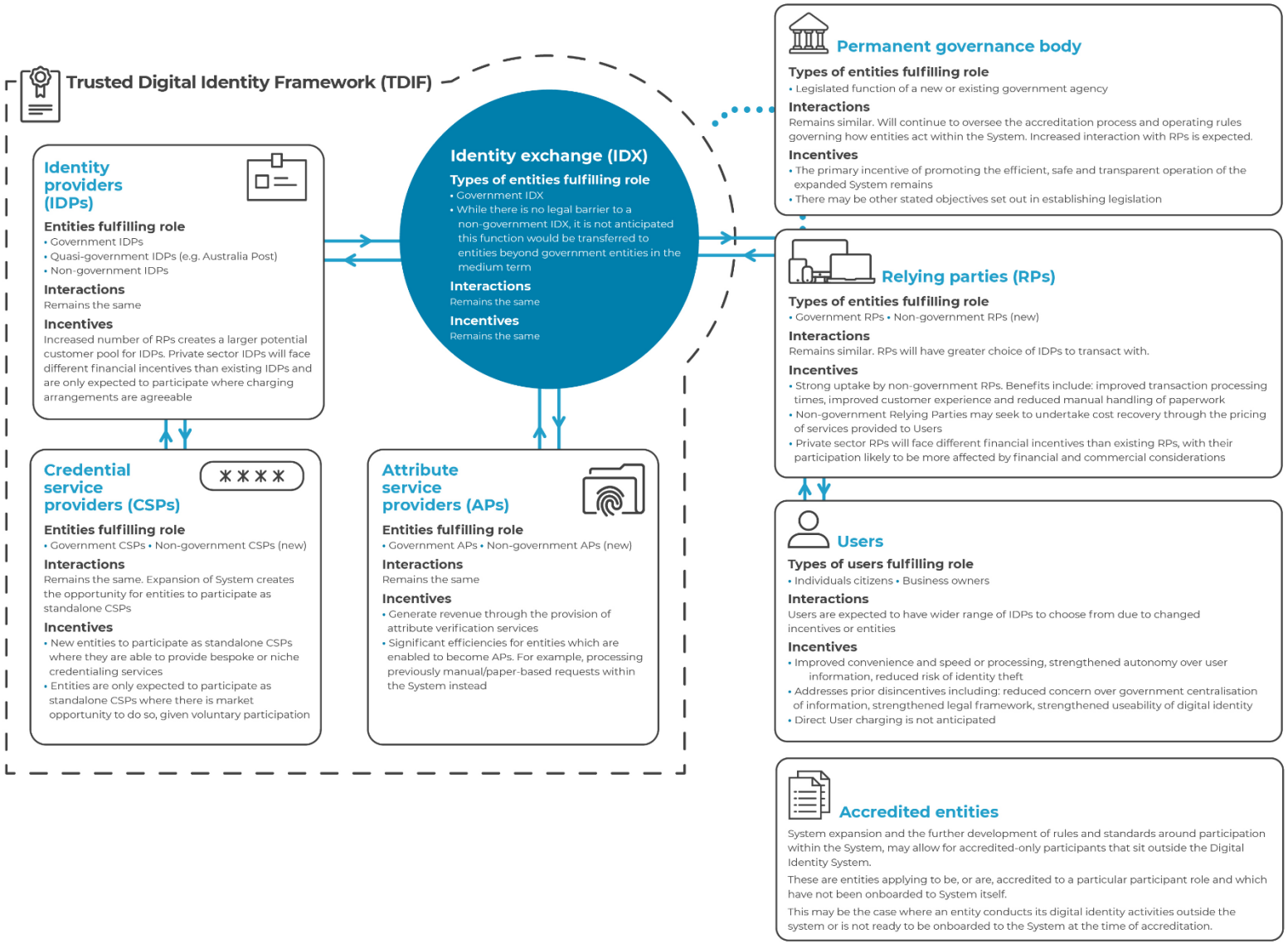


Figure 2: Entities, interactions and incentives within an expanded AGDIS

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 Digital ID system have been established. However, full realisation of its long-term benefits will only be achieved through adoption of Digital ID across the economy, eventually connecting state, territory and private sector services as well as Australian Government services. Successfully delivering the expansion of AGDIS 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 AGDIS, and are essential in building confidence for the service providers connected and citizens choosing to use their Digital ID.

Numerous studies have recognised the global potential of digital ID. McKinsey Global Institute's 2019 research paper 'Digital identification: A key to inclusive growth' found that extending full digital ID 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.

Estimates of the benefits to the Australian economy vary in scale and scope, however it is difficult to verify these. Irrespective, it is clear that Digital ID has potential for real benefits across the economy.

Research has also identified those sectors of the domestic economy which would particularly benefit from a full expansion of AGDIS capability. For example, enabling private sector participation in the AGDIS 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 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, while 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 enhancements to regulatory and policy

frameworks must 'encourage innovation'. AGDIS provides an opportunity for government to invest in a whole-of-economy business tool, which can contribute to retaining and developing a vibrant Australian RegTech sector, while 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 ID will enable the creation of new marketplaces and business models based on trusted interactions, and through them, new revenue streams".

Additionally, expanding Digital ID could deliver time savings and economic benefits for the FinTech sector. Currently, the FinTech sector experiences significant financial loss through identity fraud, with global financial authorities having fined businesses a record $8.1 billion for improper identity verification processes. Out of 94 Australian FinTech companies surveyed in 2020, 59 per cent believed that digital IDs would deliver cost savings at a projected average of $124,700 per annum. These savings would be attributable to time saved from internal identity verification processes and fraud reduction (source: Ernst & Young, 2020*, Fintech Australia Census 2020: Profiling and defining the FinTech sector*). This translates to potential savings of between $50–$100 million per annum for the sector, which currently has around 800 active companies (source: KPMG, 2020, More than 100 FinTechs added to the FinTech landscape). This data has led to a prevalent view within this sector that where FinTech companies seek to capitalise on digital ID solutions, Australians' traditional interactions with financial and banking services can be improved (source: Stellar, D 2021, Digital identity the next frontier for FinTech innovation).

3.2 Potential barriers to realising whole-of-economy benefits

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

- no legal basis for participation of non-Commonwealth agencies as relying parties, nor for a charging framework
- lack of trust in privacy and security safeguards of Digital ID
- interim, non-legislative governance framework.

There are also additional competition and market concentration risks that may reduce the realisation of benefits. These will be continually assessed as future phases of AGDIS are developed.

3.2.1 No legal basis for participation of non-Commonwealth 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 Digital ID's whole-of-economy value. While non-Commonwealth agencies can currently become onboarded accredited entities (for example, Australia Post's Digital iD solution – which is accredited but not onboarded), legislative authority is required to include non--Commonwealth agencies as relying parties (except in limited circumstances).

Without the legal authority for participation of these entities as relying parties, AGDIS 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 efficiency benefits and limit the growth and innovation of industry segments such as FinTech and RegTech. It would also not address the Murray inquiry's conclusion that a whole--of-economy solution is necessary, where public and private sector identity providers compete to supply trusted digital IDs to individuals and businesses.

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

This problem presents a fundamental obstacle to Digital ID expansion across the economy, and therefore impacts a broad range of stakeholders who would potentially benefit from such expansion, including current and potential 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 expansion beyond AGDIS.

3.2.2 Lack of trust in privacy and security safeguards

AGDIS has been designed and built with a central focus on privacy, security and consumer protection. Notwithstanding this, an expanded Digital ID market 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 using Digital ID.

Privacy and security by design

Digital ID under AGDIS 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 ID, personal information is securely encrypted and protected by strict Australian Government security protocols. Additionally, the TDIF framework governing the use of the Digital ID currently includes a range of AGDIS-specific privacy and consumer protections for individuals. These include:

- restrictions on the creation and use of a single identifier
- 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 existing requirements unless they are also contained in other applicable legislation or regulations. This is a manageable state of affairs when all participants are Australian Government entities but is not sustainable if Digital ID were to expand to encompass other accredited entities.

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, Australian Government Agencies 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 AGDIS-specific legislative requirements, the legal obligations applying to a participant's activities within the AGDIS are dependent upon whether 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: OAIC 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.

Potential inconsistencies in legal obligations applying to participants

Whilst the above privacy and security protections have provided appropriate coverage for the limited use and participants to date, expansion to non--Commonwealth agencies may result in inconsistent legal coverage. Expanding to a whole-of-economy Digital ID, including AGDIS and the accreditation scheme, 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 IDPs, IDXs and APs 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 Digital ID. 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 AGDIS participants, it is preferable that privacy protections apply as uniformly as possible.

This problem particularly affects 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 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 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 Digital ID. Of particular significance, it noted, was the fact that incorporating key privacy protections into law 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, with protection of personal information cited as a paramount consideration in business' and individual's digital activities (source: McKinsey Global Institute, 2019, Digital Identification: A key to inclusive growth). Polling by the OAIC in 2020 found that 97 per cent of Australians consider privacy important when choosing a digital service and 87 per cent of Australians want more control and choice over the collection and use of their personal information. A majority (66 per cent) of Australians were found to be reluctant to provide biometric information to a business, organisation or government agency. This wariness is not limited to potential commercialisation of personal data. OAIC's survey also found that only 36 per cent of Australians are comfortable with their personal information being shared between government entities, and only 13 per cent are comfortable with businesses sharing their information with other organisations.

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). The risk posed by this criminal behaviour has increased during the COVID-19 pandemic, with figures released from the Australian Consumer and Competition (ACCC) in August 2020 showing identity theft was up 55 per cent 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 ID, which requires sharing of personal data, including biometrics. (Internal Program research has validated the high priority that individuals place on reassurance that their information is safe and secure, and proactive security monitoring.) If AGDIS is to retain public trust whilst it expands across the economy, realising 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 Digital ID 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 AGDIS to expand beyond non-Commonwealth 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 Digital ID is likely to encourage greater participation from private sector onboarded accredited entities and, for the first time, support the participation of non-Commonwealth relying parties. Without making corresponding amendments to the current governance framework, greater participation 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 AGDIS may lead potential non-Commonwealth participants (in their capacity as onboarded accredited entities or relying parties) to doubt its long-term viability, and therefore impair uptake.
- **Enforceability** – the AGDIS 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 AGDIS 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 Digital ID.
- **Independence** – the Interim Oversight Authority is structurally independent from other participants in AGDIS but comprises officials from two Australian Government agencies who have policy and operational roles. To ensure trust in the Digital ID and its governance model as expansion occurs, it is important that independence of the oversight body increases commensurately with the scale 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 as it expands beyond Australian Government agencies.
- **Accountability** – while the AGDIS Governance Agreement imposes reporting requirements on participants and the Digital ID 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

AGDIS and accredited entities, 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 provide Digital ID services. 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 inquiry specifically identified fragmented governance arrangements as a contributor to the initial 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 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 rules and take enforcement action when breaches occur. Without a strong governance framework there is heightened risk that Digital ID will not operate as intended, resulting in potential low levels of public trust and a resultant reduction in uptake of digital identification and online services.

The Program's achievement of whole-of-economy outcomes, stimulation of innovation and economic development is reliant upon broad participation in the market – from individuals, onboarded accredited entities and relying parties - among other key actors. Expanding the AGDIS 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 to make the required investments and participate.

Stakeholder consultation conducted over a number of years has reinforced the importance of a robust governance framework entrenched, ideally, through legislation. The Program's PIA process in relation to AGDIS commenced in 2016, and saw numerous stakeholders raise 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 2016, progress has been made between states, territories and the Australian Government towards establishing a National Digital Identity Roadmap. One of the aims of this is to understand the customer experience across the range of potential digital ID systems and what will be needed from a governance and oversight perspective to ensure the systems and any customer transactions are proactively managed 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 AGDIS 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 ID

The leading role taken by the Australian Government in delivering an economy-wide Digital ID solution is legitimate, as government is best-placed to facilitate public-private sector collaboration in this area. The Murray inquiry observed that previous industry-only attempts to manage and innovate on issues of identity have shown little success, and cited digital ID 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 inquiry 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, countries like the UK, Belgium and Germany offer comparable private-public sector model use cases, with Belgium having achieved greater than 30 per cent adoption of their digital ID initiative within 5 years. Source: Internal Program research, 2021).

Governments can also lead and coordinate investment in the underlying infrastructure, systems and processes which enable an effective national approach to Digital ID, 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 ID technology, while prioritising the protection of individuals' privacy.

4.2 Government's regulatory role and capacity

Having delivered AGDIS, 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 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 ID, and the regulatory options it has available, the Government is well positioned to ensure any expansion of the use of AGDIS 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 ID, while ensuring accessibility and positive user experiences for all citizens. Comparable international examples where governments have introduced digital ID 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 ID and 'attributes trust framework' including the introduction of a new legal framework.)

The Australian Government's Data and Digital Strategy notes the use of a robust Digital ID framework will enable simpler and safer ways for people to access public services and provide more secure ways to share data across jurisdictions. This alignment suggests government intervention has already commenced and can be sustained and enhanced to support 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-Commonwealth agencies as relying parties, nor for a charging framework.	Government action enables expansion of the AGDIS to include non-Commonwealth agencies as relying parties, and providing a legal basis for charging by onboarded accredited entities (Commonwealth and non-Commonwealth), maximising the benefits.
2	Inconsistent privacy and security safeguards may become increasingly problematic as AGDIS 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 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 AGDIS and the accreditation system is based. These are:

- **Voluntariness** – ensuring that creation and use of a digital ID 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, 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, 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 AGDIS design
- **Integrity** – ensuring that an appropriate governance structure is in place, with an Oversight Authority responsible for operational assurance, as well as safety, reliability and efficient operation.

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 ID is the complexity of this subject matter and the low familiarity and exposure of the community to this concept and AGDIS to date. This apparent low level of public understanding could lead to any Australian Government regulation in this area to be misconstrued or viewed with hesitation and distrust.

Internal research undertaken by the Australian Government indicates that most Australians do not have a strong understanding of Digital ID. In February 2019, a 12-month assessment of user insights found that most individuals did not understand the concept or value of digital ID and were seeking more information regarding learning and trusting the AGDIS 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 ID 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 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, AGDIS 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 2006–07 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 ID is and is not. Under the proposed approach, a digital ID 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, 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 AGDIS 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 ID, enabling its expansion, entrenching privacy and other consumer protections, and establishing permanent governance arrangements. This would be regulated an independent Australian Digital ID Regulator (initially the ACCC).

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 AGDIS entities, interactions and incentives described in Section 2.3.3 Entities, interactions and incentives within the current AGDIS continue. This would entail ongoing application of TDIF policy to onboarded accredited entities and continued oversight by an interim governance body. This would remain fully accessible by Australian Government relying parties only, with involvement continuing to be managed through System Governance Agreements/Memoranda of Understanding (MoUs) between Australian Government agencies. Onboarded accredited entities using Digital ID 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 Digital ID through an identity provider: the Australian Government identity solution, myGovID. Individuals can continue to transact with a select range of Government services and entities. As described above, it is not legally permitted for non-Commonwealth agencies – including businesses or community organisations – to become fully operational relying parties (except in limited circumstances). Nor is there a legislative framework for charging outside the Australian Government, practically limiting the incentives for non-Commonwealth 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 delivery. That is, continue to provide oversight, make incremental adjustments as needed to the TDIF governance framework, and manage the entry of new participants. The entry of non-Commonwealth participants, and further expansion, would be limited by the absence of legislative authority for non-Commonwealth 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 Digital ID. 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 Digital ID 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 privacy rules and requirements.

As it leverages existing regulatory arrangements, Option 2 would not be capable of providing legal authority for expansion of Digital ID 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 AGDIS and an accreditation scheme, including an established role for the ACCC as the initial Australian Digital ID Regulator. The regulatory scheme will be established through a package of instruments including the *Digital ID Bill 2023* and associated rules (the Bill), as well as further legislation covering transitional and consequential matters. Both pieces of primary legislation would become law upon Parliamentary approval, whereas the Digital ID Accreditation Rules and Digital ID Rules are legally binding instruments which must be tabled in, and can be 'disallowed' by, Parliament. Various other documents will give operational effect to the regulatory scheme, including technical standards which will be legislative instruments not subject to disallowance.

Option 3 supports an expansion of Digital ID, by providing both the legislative authority to involve non-Commonwealth 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 AGDIS and accredited providers (not digital ID systems in general, though other digital ID 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 and relying parties, with economic incentives in place for private sector engagement, 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, the Australian Government's position on each of these areas has been informed by ongoing analysis and consultation inside and outside the Government, including release of an exposure draft Bill. The most recent consultation

sought direct feedback on the Digital ID Bill and the Digital ID Rules which outline the proposed regulatory framework and regulator establishment.

Application of regulatory scheme

Under Option 3, legislation would enable Australian Government, state and territory entities (including local governments) and private entities to connect to AGDIS to offer or use digital ID 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 Digital ID 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 ID – regulation stops once the relying party has received verification of the person's digital ID.

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 Services Australia as the system administrator, the ACCC as the initial independent regulator, and the OAIC. The extent to which regulatory requirements apply is dependent upon what is appropriate given the 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 AGDIS, usually only the 'core attributes' for a digital ID.

Features of regulatory scheme

As set out in the Bill, it is proposed that under this dedicated regulatory scheme, the implementation and operation would become a legislated function of the ACCC, supported by a system administrator being Services Australia. 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 ID (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 ID. (Where the term "digital ID" is used in the context of Option 3, it can be assumed that this refers to the term as defined in legislation. In other sections of the

document, “digital ID” has the meaning set out in the Glossary at Attachment A).

- Establishment of an Establishment of a Regulator to oversee AGDIS and the accreditation scheme. There is also a role for a system administrator and the Information Commissioner
- to oversee AGDIS and the accreditation scheme – the Oversight Authority.
- Obligations for accredited entities (i.e., entities not using the AGDIS).
- The ability of the Minister to appoint advisory committees.
- Applications for accreditation and onboarding and related matters.
- Notice of decisions.
- Internal and Administrative Appeal Tribunal review of decisions.
- Registers to show entities that are participating or are accredited .
- Privacy and other consumer safeguards, security and fraud-prevention requirements applying to participants in a digital ID system.
- Compliance powers.
- For participants:
  - the ability to establish a charging framework
  - a liability 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.
- A trust mark framework with a civil penalty for unauthorised use by a person.

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

Further detail on the regulatory measures contained within Option 3 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 Option 3 would enable the introduction of a 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 AGDIS by participants.

The framework will not directly impose charges on individuals using Digital ID but also will not regulate fees charged by relying parties wanting access 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 charging framework has continued throughout 2023, 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 Program consultation conducted is described in more detail at Section 10 Consultation.

Mitigating regulatory impact

A key feature of Option 3, reflected in the Bill, 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 Bill (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 specific terminology and concepts that are already established within sources such as the TDIF and National Identity Proofing Guidelines, under the accreditation system. This will be of particular benefit for entities which are already participating or interacting prior to the legislation being passed
- the adoption of 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 of 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 Impact Analysis 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, by selecting an identity provider and using their Digital ID to transact with available services online. Individuals who are potential users are also considered.
- **Businesses** – refers to private sector entities who may wish to be accredited or participate. The impacts of each policy option will differ depending on businesses' intended form of participation, their level of digital maturity, 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 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.

6.3 Regulatory impacts

Regulatory costs form a subset of the overall impacts (costs and benefits) of Digital ID. 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, this Impact Analysis calculates the estimated regulatory burden for Options 2 and 3 (noting that Option 1, as the status quo, presents no regulatory burden). The approach to determine this is set out below with further information on the costing methodology provided at Appendix E.

6.3.1 Regulatory costs

Under the Regulatory Burden Measurement Framework, only certain costs associated with the Digital ID 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 are not quantified under this Impact Analysis.

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 focuses on regulated entities only. Stakeholders to which regulation would apply, and therefore the focus of this regulatory cost analysis, are:

- **Accredited entities –** Entities accredited for a particular role which have not been onboarded.
- **Participating (onboarded) entities** – Entities that are accredited and onboarded to the Digital ID System as either Aps, CSPs, IDXs and/or IDPs.
- **Relying parties** – Rely upon verified information provided through AGDIS or an accredited provider 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 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 future (with Australia Post's identity solution already accredited), these types of entities are included in the regulatory burden measurement.

6.4 Impact analysis approach

The impact analysis has been progressed iteratively alongside the policy development process, and reflects feedback received as recently as October 2023.

Initially, it focused upon identifying broad *categories* of anticipated costs and benefits arising from the proposed policy options. A comprehensive scan was conducted of available literature and evidence on the impacts Digital ID – 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 ID 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 ID programs in these different country contexts were 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 AGDIS, which were then excluded from analysis. For example, in India one of the most significant benefits of digital ID'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.

Further, consultation conducted by the Program also supported the identification of potential costs and benefits arising from this proposed regulation. Submissions to 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 regulatory scheme).

In October 2021, the identified impacts of all options (both qualitative and quantitative regulatory cost estimates) were validated through public release of the Consultation Impact Analysis. The outcomes of this and other consultation activities are discussed in more detail in Section 10 Consultation.

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 AGDIS 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 AGDIS through myGovID (the Australian Government's digital ID provider), and transactions within it continue to be limited to Commonwealth (and select state and territory) 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 135 digital government services currently accessible. However, the exclusion of non-Commonwealth agencies as relying parties (except in limited circumstances) and charging onboarded accredited entities under the status quo constrains the places and contexts in which individuals can use AGDIS.

The implications of the status quo arrangement for individuals are two-fold. First, 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 AGDIS currently (primarily Australian Government). Second, the full efficiency benefits for individuals cannot be realised due to ongoing inability to expand to the private sector. Legislation is required to bring non-Commonwealth relying parties and charging onboarded accredited entities, 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 AGDIS as relying parties nor as onboarded accredited entities with a legislative ability to charge, future growth in the number of participants entering as onboarded accredited entities (for example, as IDPs or Aps), may also be inhibited. While AGDIS 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 Digital ID services.

Individuals who use the AGDIS incur no direct costs, as their use 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 with available Government services. However, they would forego the additional or compounded benefits that would arise from the expansion to non-Commonwealth 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 interact regularly 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 as relying parties
- increased choice and control in how they engage with Digital ID – 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 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 ID. This leads to an overall net positive benefit for individuals, compared to a situation where AGDIS is not available. However, considered in relative terms the net benefits of the status quo for current and potential individual users are lesser than those available under other options that may enable expansion.

7.1.2 Businesses

Under the status quo, small, medium and large enterprises face no regulatory costs because their participation in AGDIS 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 enter the market – 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. 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 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, forego all benefits expected to accrue under a dedicated regulatory scheme. These include:

- Efficiency and potential for 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 that 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 in terms of the efficiency and productivity gains. However, under this option, a significant number of businesses are unable to participate 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 scheme. This means that on a relative comparison, the net expected benefits for business of the status quo are likely to be less than under other options.

7.1.3 Government

While continuing the regulatory status quo arrangement may offer some certainty for government stakeholders, 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 its approach to Digital ID expansion. 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 is inherently limited.

Currently, Australian Government entities participating in AGDIS 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 approach to Digital ID)
- 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. If state, territory and local governments are unable to participate, 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 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, as they are largely excluded from participation. As with businesses and government entities that 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. If Australians collectively trust AGDIS 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 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 AGDIS 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 AGDIS continues operating with no dedicated legislative or regulatory framework, it presents no regulatory impact. Even if there

were, the ongoing restrictions on non-Commonwealth involvement under this option means that such regulation 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 Digital ID System for stakeholders, the status quo arrangement continues to confer notable benefits on current Australian Government agency participants, some businesses, and Australians – insofar as access 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 through other options canvassed in this Impact Analysis. Under the status quo, there are no additional or changed regulatory costs incurred by any stakeholders.

Despite the many proven benefits of AGDIS, 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 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.

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

As with Option 1, Option 2 supports involvement from Australian Government agency participants only and Australian individuals. However, this option will not support an expansion of to non-Commonwealth relying parties, nor provide a legislative charging framework for use by non-Commonwealth 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 benefits gained from interactions with current Australian Government agency participants. 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 ID. 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 AGDIS services, they would continue to benefit from the indirect time savings attributable through reduced time required to present identity documents, set up multiple identity profiles across diverse service providers and verify their identity with service providers. Economic modelling has indicated that, on a per transaction basis, this can be quantified as 115 minutes of time saved from completing a transaction using digital id compared to without, equivalent to **$61.00 per transaction** (using the default value for an individual's leisure time per the Regulatory Burden Measurement Framework), noting that this figure does not represent a cost saving as it is not directly attributable to Option 2.

Extrapolating this per-transaction benefit across the economy, using the estimated transactions through myGovID in 2021–22 as a basis, the whole-of-economy transaction savings are estimated at $3.312 billion across 54 million transactions. These figures are conservative estimations that account only for government transactions and do not incorporate any increase in volume across the years. It is possible that AGDIS accompanied by legislative privacy protections, enhanced trust and confidence as a result of this option would increase uptake by individuals, and thereby increase the volume and significance of time savings benefits to individuals across the economy.

However, Option 2 is not expected to substantially increase the range of agencies or entities participating 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 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 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 less.

8.1.2 Businesses

Option 2 would not alter any of the existing legal barriers preventing participation by businesses. 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 fewer 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 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.

Relying parties

Option 2 does not address the existing restrictions on businesses participating in the as relying parties. Businesses which are potential participants would therefore not experience regulatory costs due to being excluded from participation. 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 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 market of more onboarded accredited entities, which 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 less for businesses than under Option 3.

8.1.3 Government

Option 2 does not affect the range of government entities which can participate. 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 most Australian Government participants currently operating a service. 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.

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 AGDIS. The approach may introduce added complexity for implementation and operation on an ongoing basis. The source of AGDIS' 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 cost 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 Government decisions 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 market 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 less than that available under Option 3.

8.1.4 Community

Option 2 does not address the existing restrictions on community organisations' participation as relying parties or as onboarded accredited entities with a legislative ability to charge. As such, community organisations that would otherwise wish to participate 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 understanding of Digital ID, and 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 may be slightly improved by Option 2, due to increased privacy and security protections. However, trust and confidence 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 of non-Commonwealth 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 (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 within the Framework's scope. Under 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 Digital ID System's privacy and security safeguards, the primary shortcoming that 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 universally, consistent obligations across all using entities, 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 Option 2 is expected to be negligible. As participation is voluntary for GBEs and other participants, it would be expected that GBEs only would only provide services if these regulatory costs were offset by broader economic and commercial benefits available.

The regulatory cost for Option 2 is the estimated total amount it would cost impacted entities to comply with leveraging existing regulatory systems to enhance privacy safeguards, based on time and labour costs to undertake required activities (i.e. it is not a 'fee' or 'charge'). This figure has been developed in accordance with the Australian Government's Regulatory Burden Measurement Framework, and relies on a range of assumptions described in further detail in Appendix E Regulatory costs: Methodology and assumptions. The annual economy-wide regulatory cost of Option 2 has been estimated at **$23,502**, as set out in Table 3 below. For contextual purposes, the select indirect benefits estimated at a whole-of-economy level from individual time savings are also presented below in Table 4.

Option 2 Average Annual Compliance Costs (from business as usual)

Costs ($m)*	GBE**	Business	Community Organisations	Individuals	Total Cost
Relying Parties	$23,502				$23,502
Total by Sector	**+ $23,502**	N/A	N/A	N/A	**+ $23,502**

Table 3: Option 2 Regulatory burden estimate (RBE) table

* **Costs ($m)** are average annualised economy-wide costs calculated over the default 10 years of regulation required by the Regulatory Burden Measurement Framework.

** This assumes that all **GBEs** will onboard as relying parties over the first four years until all (currently nine) are onboarded. As such, the compliance costs increase each year before plateauing from years five to 10.

Option 2 Select Indirect Benefits^ (from business as usual)

Benefits*	Number of transactions**	Business	Community organisations	Individuals	Total change in benefit
Individual time saving	1			115 minutes	115 minutes

Individual transactions saving	1		$61.00	$61.00
Whole-of-economy transactions savin	**54,000,000****		**- $3,312,000,000**	**- $3,312,000,000**

gs				

Table 4: Option 2 Select indirect benefits table

^ Indirect benefits may be realised by individuals, businesses and community organisations as regulation fosters additional service offerings and options for verifying identity. It is expected that an individual could save 115 minutes of time (source: KPMG, 2021, Economic Benefits of Digital Identity) by completing a transaction with a digital ID compared to without. Based on the default value for an individual's leisure time ($32 per hour per the Regulatory Burden Measurement Framework), this would equate to an individual benefit of $61.00 per transaction. Similarly, for a small business it is expected that setting up an ABN and registering a business name would take a quarter of the time it would otherwise. Estimated to save the business $128 in this transaction. However, these are time savings not cost savings and are not directly attributable to the regulation. Rather, they are a result of an additional identity verification option becoming available.

* Please note, the savings quantified in the above table are not comprehensive as there are other benefits to businesses, community organisations and governments as described in Section 8.1. The savings detailed in the above table have been calculated as follows:

Individual saving per transaction ($61.00) x number of transactions

** The number of transactions used in this calculation is based on estimated transactions through myGovID in 2021-22 used in the Digital ID Charging Framework. This is based on government transactions only and is a conservative estimate as it does not incorporate any increase in volume across the years and does not include transactions that may occur through uptake of private sector services. Private sector take-up impacting the volume of transactions cannot be accurately forecast as it is dependent on a number of factors, including the future charging framework.

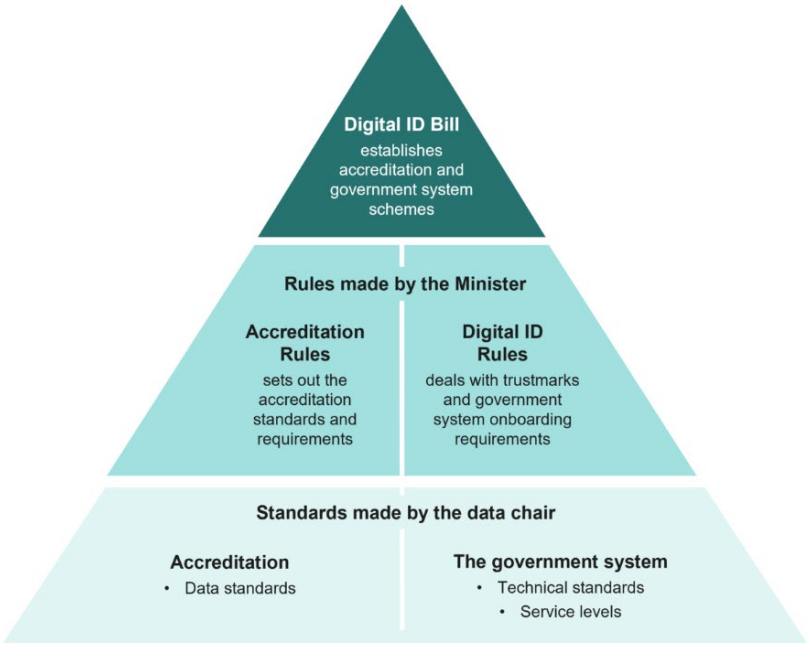
8.3 Likely net benefit

The above analysis concludes that Option 2 may offer some efficiency and productivity benefits for select stakeholder groups that already have legislative authority to use Digital ID under existing arrangements – notably, individuals (primarily in the form of time savings) and governments. This is offset by minor regulatory costs incurred by a very narrow category of users (specifically GBEs) which are expected to be minimal given these entities' existing obligations to comply with Privacy Act regulations. 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 through expansion to include non-Commonwealth relying parties, under a dedicated regulatory arrangement.

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, Option 3 involves establishing a dedicated regulatory scheme that would support an expansion of AGDIS to include an accreditation scheme. This option would, through the Bill, provide legislative authority to involve non-Commonwealth relying parties, and the ability for onboarded accredited entities to be subject to a legislated charging framework.

The regulatory framework has three core functions in its structure; the establishment of the accreditation system and AGDIS, the ability for the Minister to make accreditation rules and rules for governance of AGDIS, and data standards made by a data chair. This provides not only the legal basis for operation, but the ability to respond to regulatory concerns, and shape the market as it grows and evolves.



9.1 Overall impacts

9.1.1 Individuals

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

- indirectly from the expansion enabled by the legislation.
- 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 Digital ID 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 ID 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 accreditation has also been received from international IDPs wanting to offer digital ID 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 has indicated that an individual could save 115 minutes of time just by completing a transaction with a digital ID compared to without (source: KPMG, 2021, *Economic Benefits of Digital Identity*). This would amount to an individual time savings benefit of $61.00 per transaction (using the default value for

an individual's leisure time per the Regulatory Burden Measurement Framework), noting that this figure does not represent a cost saving as it is not directly attributable to the regulatory scheme but, rather, is an indirect benefit.

Extrapolating this per-transaction benefit across the economy, using the estimated transactions through myGovID in 2021–22 as a basis, the whole-of-economy transaction arrive at approximately $3.312 billion across 54 million transactions. These figures are conservative estimations that account only for government transactions and do not incorporate any increase in volume across the years or potential uptake of private sector services (which cannot be accurately forecast at this stage, being dependent on several factors). However, it may be assumed that an expansion of Digital ID supported by a regulatory scheme would only allow for an increased volume in these transactions across additional service offerings and options for identity verification, which would thereby increase the significance of time savings benefits to individuals across the economy. Consultation and consistent engagement with the Australian public would be a crucial factor in allowing for optimal realisation of these benefits for individuals, an insight that can be drawn from the UK digital ID experience. Research indicates that a key challenge to private sector and broader uptake of GOV.UK was that the public did not feel well informed about digital ID and biometrics, with consultation revealing that more than half of those engaged felt that they were either not well informed or knew nothing about the issues surrounding the UK program. (Source: Biometric Update.com, 2021, Government Digital Identity Plans Advance Amid Scepticism, Lack of Awareness)

These select time savings would be expected to grow as the range of places individuals can use Digital ID expands.

The accreditation system to allow private sector participants is also expected to confer benefits for individuals in relation to the avoided costs of data spills and associated identity theft and fraud. The World Bank previously estimated worldwide identity theft costs to be at least $307 billion per annum, with $8.3 billion resulting from credit and debit card fraud. It noted that a robust identification system with efficient query mechanisms, customer identification, and high levels of integration could help significantly combat these figures (source: World Bank, 2018, Private Sector Economic Impacts from Identification Systems). An expanded program offers such a solution, providing for a higher standard of secure verification and reducing the need for physical identity documents.

With a significant amount of identity fraud occurring in relation to transactions with banks and other financial services providers, the expansion to these providers presents a meaningful opportunity to reduce the individual costs of this kind of crime. As with the time savings benefits, the avoided costs of identity fraud and data spills would be expected to grow as the number of private sector providers adopting Digital ID 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 Digital ID 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 Digital ID 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 through the legislation.

The regulatory scheme will enhance privacy protections for individuals. The proposed protections would represent a strengthening of those currently 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 security and integrity rules on AGDIS and Accreditation Scheme participants, 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 over how and when they interact with Digital ID. 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 ID, 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 Digital ID may be charged to do so by a relying party. Given the voluntariness approach, and the requirement that alternatives remain available, relying parties would need to ensure that such charges are set at a level which incentivises individuals to use Digital ID, 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 ID. However, this does not appear to be a significant risk considering the balance of costs and benefits for these participants, discussed below.

Assessment of net expected benefits: Considering 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 under Option 3 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 several different contexts. Under the status quo, businesses can already become an onboarded accredited entity (but are unlikely to be active due to the absence of a charging framework), 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 to provide verification services relating to qualifications.

Businesses participating 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 as accredited entities that choose not to be onboarded, or as relying parties. For example, utilities providers may connect with one or more IDPs to undertake identity verification on new customer accounts. Businesses participating 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, accredited entities or relying parties. As accreditation and participation is voluntary for businesses, it is expected that only those organisations which perceive a net positive benefit will choose to participate.

Onboarded accredited entities

(a) Expected benefits of regulatory scheme

Currently, private sector entities wishing to participate as onboarded accredited entities are not supported by a robust system of regulatory safeguards and frameworks. For businesses considering making investments necessary to participate, Option 3's 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 also establishes the framework and principles for a charging scheme associated with use of Digital ID. The details of this scheme 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 scheme provides a basis for onboarded accredited entities to generate significant commercial benefits through the aggregation of fees received as a service provider. The exact quantum of these benefits will be determined by the regulatory scheme's charging framework.

The regulatory scheme will strengthen safeguards for non-Commonwealth agencies participating. 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 rules and regulations. This would significantly mitigate the risks of service provision, compared with the status quo in which such protections are not available to non-Commonwealth agencies.

Further, private entities that currently provide digital ID services as part of their commercial offering, such as credit and background checking agencies will benefit from the possible evolution of their service offering – supported by the new regulatory scheme. This demonstrates Option 3's capability to not only facilitate the creation of new digital ID 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 Digital ID--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 as onboarded accredited entities are anticipated to be larger private sector businesses. As previously noted within this Impact Analysis, 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
- AGDIS and infrastructure security requirements established to meet the standards of accreditation
- compliance monitoring to ensure 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.

It should be noted that some of these costs would be incurred in the development of any private sector digital ID product or solution, regardless of whether it is regulated by the Government. It should also be noted that joining as an onboarded accredited entity is entirely voluntary, so businesses that assess the costs of compliance as outweighing the specific benefits for their organisation can 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 some information about individuals, and the regulatory scheme contains specific restrictions on the on-selling or use of customer data collected through Digital ID. 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.

Accredited entities

(a) Expected benefits of regulatory scheme

For entities seeking accreditation under the TDIF but not onboarding, the benefits and costs are slightly different. As with onboarded accredited entities, private sector entities wishing to participate as accredited entities are not currently supported by a regulatory scheme. Option 3 will establish a nationally consistent and recognised approach to accreditation by mandating strict standards and validating all entities that have been accredited with a Trustmark.

The key benefits to accredited entities come not through participation but through commercial opportunities generated and enhanced by the Trustmark. This allows an accredited entity to convey to a potential service provider or citizen that they meet the trusted and high standards set by the Australian Government, assuring the security and trustworthiness of their digital ID services (notwithstanding that they are not provided through AGDIS). This would be a particular advantage for small, medium or regional businesses, who could indicate to the digital ID market, including entities onboarded with which they may still transact with, that they meet the same standards as their larger and more mature market competitors, offering them an economic advantage.

(b) Expected costs of regulatory scheme

The legislation will require accredited entities to adhere to several requirements in order to achieve and maintain accreditation. Some of these align with those described above for onboarded accredited entities, including privacy and consumer safeguards and rules around the use of Trustmarks. However, as accredited entities are not onboarded, they are not required to comply with additional requirements that relate to engaging with Digital ID-related activities or measures.

Importantly, accredited entities would not be able to directly benefit from the establishment of a charging regime, unless/until they decide to onboard. The scope of legislation under Option 3 only establishes a charging framework for those onboarded. As noted above, entities may assess the costs of compliance against the specific benefits for their organisation and choose whether or not to join at any time. Accredited entities may find that the opportunity cost associated with not participating, incurring the benefits determined by the charging framework, may lead businesses to eventually choose to onboard and participate.

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 AGDIS and accredited providers. 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, due to 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 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 Digital ID to complete business set-up tasks with government entities. The productivity benefits associated with expanded access for *all* kinds of transactions across multiple sectors, including verification of customer identities, could 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, including by relying parties. This means that businesses which seek to use Digital ID solutions 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 ID 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, such as a suspected fraud or cyber security incident.

The extent of costs imposed on relying parties by 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 Digital ID 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. Entering the Digital ID market 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 charging regime, an indirect consequence is that relying parties will face future charges for using services 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 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 because 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 accreditation and participation are 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 delivering the Program, as well as in drafting and enacting legislation and subordinate regulations supporting its expansion.

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 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 AGDIS– by enabling reduced paperwork, faster transactions and improved convenience – will generate significant gains in administrative efficiency. Digital ID 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 reduced requirement for agency-specific identity, access management services and subsequent support systems.

The use of the AGDIS is expected to support state and territory government services across:

- the registration of births, deaths and marriages
- state and local government licensing regimes
- school, vocational education, and training and higher 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 can use Digital ID in place of paper-based and face-to-face identity verification.

Governments will also benefit from a reduction in identity fraud in an expanded Digital ID, through fewer 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 use of AGDIS.

Additionally, as legislation will support an expansion 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 ID platforms or may no longer need to develop their own solutions. The automatic de-duplication processes would also present a significant time and cost saving for these additional government entities, which 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 depends 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 due to a need to transition from or decommission existing digital ID investments and services, where such platforms are under development. However, as Digital ID 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 use.

Australian Government agencies and 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 (including state and territory governments, which currently are not subject to the NDB 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 for state and territory levels of government, where the NDB Scheme or comparable 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 to a wider range of Australian Government entities and state, territory and local governments creates the potential for very large efficiency gains in relation to identity verification. In addition to reducing manual handling of paperwork and freeing up resources to focus on more complex/meaningful service delivery work, Digital ID also allows government entities

to offer citizens a better service experience. This is expected to generate intangible benefits in terms of citizen satisfaction, staff experience and attachment which cannot be costed but will contribute to the overall benefits delivered by 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 practices. Given that most government entities are already subject to these obligations in some form, the transition costs and ongoing compliance costs are not anticipated to differ significantly from the status quo at this time. However, any state and territory governments participating as onboarded accredited entities, will face new regulatory requirements equivalent to those imposed by the NDB Scheme. Non-Commonwealth agencies will also be subject to the 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 enabled by this regulatory scheme.

9.1.4 Community

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

Legislation will enable community organisations to interact with Digital ID, 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.

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

Similarly, where community organisations participate 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 (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 and services – which, although unable to be quantified, contribute to the overall benefit to the community under Option 3. Further, community organisations in particular stand to benefit from efficiency gains and reduced manual handling.

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

9.2 Regulatory impacts

9.2.1 Overview

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. These estimated regulatory costs have been informed through the Consultation RIS, which provided a detailed list of regulatory impacts within the Bill for each stakeholder group and tested the accuracy of estimates. The regulatory impacts of Option 3 can be summarised into the categories below.

- **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 Bill provides high-level requirements for when applications must be made, with the rules outlining relevant content requirements.

- **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.

- **Ongoing obligations**: The ongoing obligations an entity is subject to because of either use of the system, or their accreditation status. This may include, for example, annual assessments and reaccreditation-related requirements (if directed by the Oversight Authority).

- **Administrative**: Various administrative requirements of regulated entities under the regulatory scheme, including recordkeeping and data retention requirements. These obligations vary given the involvement and likely data accessed and used by an entity. It is expected that some administrative requirements included in the regulatory scheme (e.g., 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.

9.2.1 Assumptions and parameters

The regulatory cost calculated for Option 3 is the estimated amount it would cost impacted entities 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 methodology by which this figure has been developed is consistent with the Australian Government's Regulatory Burden Measurement Framework, and relies on a range of assumptions described in further detail in Appendix E Regulatory costs: Methodology and assumptions.

An important assumption made in calculating the regulatory burden was that the entities seeking to participate in this regulatory scheme would already have a baseline level of familiarity with the digital ID market and a corresponding level of

maturity in their corporate systems, processes and standards. This provided a more realistic view of the additional activities required to meet regulatory requirements, than by considering entities with minimal/low digital ID maturity. In the case of such low-maturity entities, significant uplifts and changes to business practices would be required in preparation to engage with any digital ID system – whether it was regulated by government or not.

9.2.2 Regulatory Burden Estimate (RBE)

The estimated annual economy-wide regulatory cost of Option 3 is **$1,498,652**, as set out in Table 5 below. For contextual purposes, the select indirect benefits estimated at a whole-of-economy level from individual time savings are also presented below in Table 6.

Option 3 Total Annual Compliance Costs (from business as usual)

Costs ($m)*	Average number of entities**	Business	Community organisations	Individuals	Total change in cost***
Relying party (non-government)	215	$703,577.00			+ $703,577.00
Accredited entity (non-government)	28	$484,732.00			+ $484,732.00
Onboarded accredited entity (non-government)	22	$310,342.00			+ $310,342.00
Total by sector		**+ $1,498,652.00**			**+ $1,498,652.00**

Table 5: Option 3 Regulatory burden estimate (RBE) table

* **Costs ($m)** are average annualised economy-wide costs calculated over the default 10-years of regulation required by the Regulatory Burden Measurement Framework.

** Assumes an uptake of relying parties and accredited entities increasing each year over the 10-year timeframe (see Appendix E for further details), before plateauing from year four onwards. The table above provides the average number of affected entities over the 10-year timeframe of regulation calculated. The total costs for each entity type are impacted by the number of entities.

*** Please note, this is not a per entity cost, rather an economy-wide cost based on the number of entities impacted.

Option 3 Select Indirect Benefits^ (from business as usual)

Benefits*	Number of transactions**	Business	Community organisations	Individuals	Total change in benefit
Individual time saving	1			115 minutes	115 minutes
Individual transaction saving	1			$61.00	$61.00
Whole of Economy transaction savings	**54,000,000****			**- $3,312,000,000**	**- $3,312,000,000**

Table 6: Option 3 Select indirect benefits table

^ Indirect benefits may be realised by individuals, businesses and community organisations as regulation fosters additional service offerings and options for verifying identity. It is expected that an individual could save 115 minutes of time (source: KPMG, 2021, Economic Benefits of Digital Identity) by completing a transaction with a digital ID compared to without. Based on the default value for an individual's leisure time ($32 per hour per the Regulatory Burden Measurement Framework), this would equate to an individual benefit of $61.00 per transaction. Similarly, for a small business it is expected that setting up an ABN and registering a business name would take a quarter of the time it would otherwise. Estimated to save the business $128 in this transaction. However, these are time savings not cost savings and are not directly attributable to the regulation. Rather, they are a result of an additional identity verification option becoming available.

* Please note, the savings quantified in the above table are not comprehensive as there are other benefits to businesses, community organisations and governments as described in Section 9.1. The savings detailed in the above Table have been calculated as follows:

Individual saving per transaction ($61.00) x number of transactions

** The number of transactions used in this calculation is based on estimated transactions through myGovID in 2021-22 used in the Digital ID Charging Framework. This is based on government transactions only and is a conservative estimate as it does not incorporate any increase in volume across the years and does not include transactions that may occur through uptake of private sector services. Private sector take-up impacting the volume of transactions cannot be accurately forecast as it is dependent on a number of factors, including the future charging framework.

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, 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. Considering, for example, that an individual's time savings benefit under the status quo, has been calculated for some transactions at $61.00 per transaction, which, when extrapolated to a whole-of-economy estimation under the current arrangements only, is conservatively around $3.312 billion, the significance of potential time savings benefits that may become available under an expanded system supported by a regulatory scheme is evident. 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, 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 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 88 additional benefits of improved efficiency, additional revenue streams and reduced legal risk will be accrued.

The annual average economy-wide regulatory cost of Option 3 has been estimated at **$1,498,652**, capturing a range of expected compliance costs under the proposed regulatory scheme. These costs are expected to be borne by the small proportion of businesses perceiving benefits in choosing to engage with, and participate in, under Option 3. These costs will also be offset by the extent of a business's existing maturity level (i.e., how established technical systems/processes, privacy and security arrangements and resources are) and the effect of expected benefits per entity type. Overall, the net effect of regulatory change for businesses under Option 3

will likely see the benefits of involvement outweigh the costs of regulatory compliance.

Australian Government agencies, state, territory and local governments are likely to benefit from significant productivity and efficiency gains across their identity verification practices, allowing them to offer Australians a more positive service experience. While citizen satisfaction, staff experience and attachment cannot be quantified, 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 differ significantly 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 Digital ID 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 expansion 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 framework as an onboarded accredited entity, and voluntarily choose to undergo the accreditation process if this balance of costs and benefits is considered favourable.

Establishing a dedicated regulatory scheme through legislation is the only option which supports expansion to a wider range of public and private sector services, particularly non-Commonwealth 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 Digital ID services.

10 Consultation

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.

Australia also engages heavily with international stakeholders and counterparts in digital ID 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 ID 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. Finance continues to work with the Australian Government and with similar agencies around the world to identify future opportunities for digital ID interoperability and mutual recognition with other countries.

As Digital ID expands, supported by appropriate regulation, this domestic and international engagement will continue and increase. This consultation approach to date, and future activities described in this section, seek to fulfil two primary objectives:

- Ensuring 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 approach recognises that digital ID is a complex concept, some aspects of which may not be well understood by the community, and involves highly sensitive topics such as privacy and information security. As regulatory options were

explored, the plan flexibly ensured that the broad range of perspectives we received informed the development of policy positions, and allowed any unintended consequences to be identified.

10.2 Consultation undertaken

Consultation has been a key focus since the Program commenced, to ensure the design, operation and governance considers and accommodates stakeholder views. Since 2015, the Australian Government has engaged with the public to build a Digital ID system that is aligned with community expectations. The broad range of consultations conducted by the Program are listed at Appendix D. This consultation has occurred through a range of channels (including in person, through interactive webinars, surveys, and public submissions). Further consultation has been undertaken in late 2023 to inform the Bill, with changes made to reflect community and business expectations and feedback.

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 ID legislation. This paper sought government, community, industry, and individual views on the scope, nature and extent of possible government regulation of the Digital ID 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. 44 submissions were received through this process – 16 of which were from state and territory governments, 20 from the private sector (including industry associations) and eight from individuals and consumer groups. On 12 February 2021, we published a

consultation synthesis report that summarised key messages, themes and outcomes of this public consultation process. The synthesis report outlined near-uniform agreement on the immense value, and on some level of legislation to govern Digital ID. 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 the release of a Digital ID legislation position paper providing updated assessments of key policy positions and the nature of potential regulation. The position paper remained open for comment for five weeks, with a total of 62 submissions received. It was supplemented by a series of targeted events, including two roundtables held on 1 July 2021 for the Australian Information Industry Association (AIIA), and 13 July 2021 for the Australian Society for Computers and the Law (AUSCL). A total of around 120 stakeholders participated in these roundtables. Other targeted consultation events that occurred during July included a series of Q&A sessions held for the banking and government sectors, at which around 21 stakeholders participated. The 2021 Trusted Digital Identity Bill exposure draft consultation was open for 4 weeks.

In late 2023, an exposure draft package, which will include the updated draft Digital ID Bill, draft Digital ID Rules, draft Accreditation Rules, was released for broad-reaching consultation. The Digital ID Bill and Rules package was open for comment for a three-week period, and the Accreditation Rules open for a six-week period concluding in October 2023. This also included public webinars, targeted industry association roundtables, and broad engagement across state, territory, and Commonwealth agencies. 112 submissions were received in addition to attendees at roundtables, and the 1346 responses to a public survey.

The consultation paper released alongside the Bill on 19 September 2023 can be accessed here.

10.3 Outcomes and themes of consultation to date

This section provides a summary of outcomes and themes of consultation feedback, by stakeholder segment and consultation round. The below draws out broad themes for discussion and analysis purposes, however it is important to understand that the

Program has received a significant quantity of diverse feedback over many years across a spectrum of stakeholders. Whilst best efforts have been made to accurately describe this feedback at a broad level, there are inherent limitations in generalising or attributing discrete sentiments or themes to what has consistently been very nuanced feedback on a complex issue.

Each stage of consultation has directly influenced and shaped Program activity – both substantive decisions and planning the future consultation roadmap. For example, November – December 2020's public consultation paper round elicited several high-level outcomes and themes across different stakeholder groups. 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 were incorporated into the exposure draft package, the outcomes of which helped shape final policy positions in the Bill.

A Consultation RIS accompanied substantial public consultation, which occurred over October 2021 and received seventy submissions which engaged deeply with one or more provisions of the legislative instruments, lodged by various industry and government stakeholders as well as by individuals. Of these seventy submissions, internal sentiment analysis by the Australian Government assessed 34 per cent of responses to be broadly positive, 40 per cent neutral and 26 per cent negative. The key stakeholder groups driving the 34 per cent of positive responses were private sector entities and industry associations, both expressing strong support for the introduction of the Bill, particularly the strengthened privacy and consumer protections. Some responses viewed the Bill (and Program more broadly) as a fundamental enabler of Australia's digital economy and expressed interest in future participation in the Digital ID system.

The key stakeholder groups driving the 26 per cent of negative responses were industry associations, consumer groups, individuals and some private sector entities. These submissions brought forth questions particularly around the scope and complexity of the Bill, governance, law enforcement access and charging. These key themes and issues specific to the October 2021 exposure draft package public consultation, have been further detailed in Appendix D, along with details of the Programs' actions in response to each issue.

Over time, common themes have emerged in the feedback received from individuals, businesses, government and the broader community. Examples of these themes, and how they have been actively addressed by the Program, are summarised below. These are further described in table form in Appendix D, with detail on how stakeholders' positions have evolved over time.

- **Individuals** - Input provided by informed individuals on regulation has generally indicated tentative positivity towards the Digital ID System and its potential benefits, with expressed hesitation on matters including privacy, safety, security and other consumer impacts. Over time, this has informed the regulatory approach of including more detailed, rather than lesser, safeguards and protections in the Bill (compared to earlier regulatory approaches explored that would address the barriers to legal authority to use the Digital ID System, without legally entrenching additional privacy, consumer and security concerns). The airing of concerns from individuals has also led to certain safeguards being built into legislation, rather than being delegated to subordinate instruments – such as a legislative guarantee of the system's voluntariness.

- **Businesses** - Whilst broadly supportive of a whole-of-economy Digital ID system, feedback from the business community initially focused upon seeking clarity on the scope and application of a Digital ID system, as well as its interoperability with other existing (current and future) systems and regulation. The decision to enshrine two alternative forms of participation in the legislation with different levels of regulation (accreditation and system onboarding) was taken in direct response to this feedback. The private sector now has two options for involvement with appropriately tailored regulatory requirements. Dialogue between the Program and the business community, particularly those in relatively highly regulated sectors such as financial services and telecommunications, has also focused on alignment with other existing regulatory schemes in areas including privacy and anti-money laundering and counter-terrorism financing regulation. This has been considered and incorporated in the regulatory scheme's leveraging of existing regulatory schemes where possible to mitigate regulatory impact, as discussed above in Section 5.3.1. Another common theme amongst the business community since early consultations on potential regulation of the system has been in relation to the charging framework. This feedback, and business' emphasizing the need for certainty yet flexibility, informed the regulatory

approach of including principles in the Bill setting broad parameters for the framework's operation (for example, ensuring legislative enshrinement of important principles such as the citizen not having to pay to participate), but leaving specific details to be determined through subordinate instruments.

- **Government** - Dialogue with state, territory and Australian Government agencies has occurred in various contexts and on a range of topics including participation in AGDIS and proposed regulation. At all levels of government, common themes that have emerged in this dialogue concern alignment with existing regulatory regimes, particularly those at a state or territory level, with the legislation being modified to contain appropriate exemptions for state / territory entities which already meet a similar level of privacy protection to Commonwealth privacy standards. In addition, for agencies with a law enforcement function, another consistent theme has been the extent to which law enforcement agencies can access and use information within AGDIS. The final policy positions on this issue, as reflected in the Bill, seek to achieve a balance between providing access to law enforcement in narrow, clearly defined circumstances, and recognising the importance of restricting the use of particularly sensitive information, in order to protect user privacy (for example, biometric information may only be disclosed to law enforcement with consent or a warrant)

- **Community** – Community feedback received by the Program has been received both from non-government organisations, as well as various special interest and consumer representative groups. Through these groups, concerns regarding the practicalities of enforcing this voluntariness protection have been raised. The Program continues to liaise closely with the Australian Human Rights Commission (AHRC), the National Children Commissioner and the Attorney-General's Department, in order to address these concerns.

In addition to the above actions taken in response to specific feedback themes raised by individuals, business, government and the community, the Program has also used feedback received across all sectors to identify common areas of misunderstanding regarding Australia's Digital ID System and its regulation. This will continue to inform the Program's ongoing communications and education strategy in relation to Australia's Digital ID System, which will run alongside and supplement the ongoing consultation on future regulation described below.

The consultation held in late 2023 has led to changes to the Bill, and the associated rules to reflect privacy, to reflect changes to governance and a range of smaller changes to improve the Bill.

10.4 Ongoing consultation

Even after the Bill becomes law, it is not envisaged that consultation and its regulation would cease. 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 additional TDIF accreditation rules and data standards are made. These proposed legislative measures ensure stakeholder views will continue to be considered and incorporated into the regulatory regime as it evolves in the future and will take allow changes to be made to reflect outcomes of future evaluation activity, and recommendations from regulators and stakeholders.

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 inquiry identified the need for a whole-of-economy digital ID solution, which would help transform service delivery in Australia and generate significant opportunities for the creation of new economic value. As this Impact Analysis has outlined, a whole-of-economy solution cannot be realised unless Digital ID 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 Impact Analysis identified the objectives of government action in relation to Digital ID. These objectives align with, and seek to address, the problem areas discussed in Section 3, which currently inhibit Digital ID 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 Impact Analysis.

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 Digital ID 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 Digital ID 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 Digital ID System's whole-of-economy benefits be realised.
2 **Lack of trust in the Digital ID 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 Digital ID System-specific laws, for example

Problem area	Policy objective	Why Option 3?
		prohibitions on data commercialisation and relating to biometrics. 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 Digital ID System. While Option 2 may, to some degree, improve trust in the Digital ID 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 Digital ID System's governance.	The introduction of a permanent Oversight Authority through Option 3 will legally enshrine the Digital ID 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 Digital ID System, support the Digital ID System's integrity and longevity, and substantially increase the overall rigour offered by current governance arrangement. Under Options 1 and 2, the Digital ID 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, discussed in Section 3.2.3: choice, consent, privacy, security and integrity. For example:

- **Choice and consent**: A dedicated regulatory scheme will ensure participation remains voluntary, making certain that individuals consent to their information being collected in connection Digital ID. For those who 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 will be both legally enshrined and strengthened in practice as a central component.

- **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 AGDIS, with the likely outcome of increasing uptake.

Option 1 will continue to secure the significant benefits currently available to individuals and businesses. However, by not addressing the obstacles to expansion, it represents a foregone opportunity to maximise these benefits and further enhance the five principles of Digital ID. Individuals would be deprived of the additional choice that would come with 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 borne by a small subset of stakeholders. These regulatory costs (estimated at a whole-of-economy annual average cost of **$1,498,652**) are offset by both the voluntary nature of Digital ID, and the many benefits available to those who choose to participate or be accredited. For contextual purposes, economic analysis estimates $3.312 billion whole-of-economy indirect benefit related to individual time savings alone, under current arrangements. 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.

Additionally, the outcomes of the Program's continuous and broad-based consultation strategy, engaging stakeholders at all levels, has informed the selection of Option 3 as the preferred option. The table below details how stakeholders have viewed the three regulatory options across the span of consultations conducted.

Regulatory options	How stakeholders viewed option throughout consultation
Option 1: Status quo	The Australian Government has been engaging with the public to build a Digital ID system aligned with community expectations since 2015. Early in 2020, the Program sought stakeholder views on potential expansion and how protections could be ensured. The Program shared an initial Scoping Paper with the Digital Identity Legislation Working Group (DILWG) and with thirteen Australian Government agencies. The Program then engaged in broad public consultation between November and December 2020, through the release of the Digital Identity Consultation Paper and Background Paper, testing views on regulatory options. Both the Scoping Paper and Consultation Paper drew strong support for the expansion of Digital ID, which is only possible through legislation. Importantly, stakeholders were in near-uniform agreement on the need for legislation to govern Digital ID. This has not altered over the course of subsequent consultations. Option 1 does not address the obstacles to expansion that stakeholder feedback has consistently shown support for, nor does it entrench privacy and security in legislation.
Option 2: Leverage existing legislative frameworks to enhance privacy safeguards	As described above, stakeholder feedback from the Program's early consultation testing views on potential regulatory options to support expansion, saw support for a whole-of-economy Program with privacy and security protections entrenched in legislation. While Option 2 offers strengthened privacy safeguards when compared to Option 1, safeguards and avenues for recourse would not be supported by a consistent dedicated regulatory framework established through legislation. As a key rationale from the November and December 2020 Consultation Paper round pointed to legislation as an opportunity to enshrine these key privacy and consumer safeguards in law in order to ensure these standards cannot change without public scrutiny, this option was also ruled out by the Program as it failed to meet this important threshold for protection set by a strong majority of those engaged.
Option 3: Dedicated legislation to establish new regulatory scheme	The outcomes of continuous legislation-specific Program consultation have solidified stakeholder support for Option 3. Option 3 offers to establish a new regulatory scheme that directly addresses stakeholder concerns, and is the only option able to support whole-of-economy expansion. Submissions received in response to the October 2021 Consultation RIS, were able to validate this conclusion and confirm Option 3 as the preferred option for a wide range of stakeholders. Consultations since the November and December 2020 Consultation Paper round were focused on engaging with stakeholders to collaboratively and transparently designing a regulatory scheme that reflected the expectations and views of the broader Australian community.

Table 8: Stakeholder views on regulatory options throughout consultation

Overall, 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. Beyond this, the Australian economy's realisation of the significant economic value of an expansion 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 regulatory regime does address all key issues addressed through consultation – however given the rapid pace of technological change and challenges in regulating emerging markets, there will be an ongoing need to monitor and establish new Rules as required. The risk profile associated with this preferred Option 3, and mitigations, are summarised in the following section.

12 Implementation and evaluation of selected option

12.1 Impact Analysis status at key decision points

The RIS has followed best practice and has informed policy development, and advice, at each key decision point. The previous Consultation RIS was released in late 2022 and informed the consultation on the previous draft Bill (The Trusted Digital Identity Bill 2021). The Regulatory Burden Estimate was considered as part of this consultation and revised according to feedback from stakeholders.

Feedback from that consultation was incorporated into the First Pass Assessment, assessed by the Office of Impact Analysis (formerly Office of Best Practice Regulation) in late 2021. No final decision was made and therefore the RIS did not progress to Second-Pass Final Assessment.

A draft of an earlier version of this RIS was provided to the Minister, and subsequently Cabinet, to inform an interim decision on whether to progress with consultation on a revised Digital ID Bill. Since then, as outlined in Attachment D, the Department of Finance has undertaken additional extensive consultation to inform the development of this Second Pass Final RIS. This version of the RIS was provided to the Minister for Finance as part of the final briefing process seeking agreement to table to Digital ID Bill in Parliament. It has been developed in tandem with the consultation process, which has informed the final Bill expected to be tabled in Parliament in late 2023.

Each key decision point has been informed by a version of the impact analysis, reflecting consultation outcomes, and final analysis of the costs and benefits of each option. The final decision point will be informed by this document.

12.2 Implementation approach

Effective implementation of the dedicated regulatory scheme will be critical to realising Option 3's full benefits. Implementation planning has been underway in the Program for some time, ensuring 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.

Whilst the proposed legislation provides broad parameters, the Program is operating flexibly within these parameters to ensure the implementation solution is designed to meet user and other stakeholder needs. Continuing focus areas for implementation planning and engagement on future phases of Australia's Digital ID System include:

- cross-Australian Government engagement on the establishment, structure and operating model of the permanent Oversight Authority.
- engaging 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 developing 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.

12.3 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 in Table 12 below, including an explanation of how they are being monitored and accommodated within the Program's implementation approach, and relevant stakeholders' roles and responsibilities. For detail on the risk framework and ratings used, refer to Appendix G.

12.4 Evaluation strategy

The phased approach to Australia's Digital ID allows for natural touchpoints to assess the effectiveness of the program. The Legislation is structured to allow the Minister to make Accreditation Rules and Digital ID rules allows for future regulation to be added if new or unforeseen issues arise, or if the Program is not working as intended. The establishment of the ACCC as the initial Regulator gives it information collection powers to undertake its role, in addition to requiring a review of accredited

entities' suitability annually. These issues will be revisited, and additional impact analyses done to inform major changes to the regulatory regime, where necessary.

A key part of the work being undertaken by the Department of Finance relates to benefits realisation. This work is being led by the Digital ID Taskforce, with oversight of the Digital ID Project Board, which includes representatives from Services Australia, the Attorney-General's Department, and the Australian Taxation Office. Benefits Realisation is an ongoing function of the Digital ID Program to identify, track and provide transparency to the benefits derived. Regular reporting to Government and its stakeholders has been implemented to provide visibility of the Digital ID Program ensuring that it's meeting its intended objectives.

The Bill also includes a requirement for a statutory review two years after commencement, which will draw from data collected from the regulators, and the above cross-agency Project Board.

Challenge/risk	Likelihood	Consequence	Management	Residual risk rating	Relevant stakeholder(s) and roles / responsibilities
• **Potential for regulation to be misunderstood or distrusted, leading to low confidence levels and low uptake of Digital ID.**	Likely	Severe	Clear and strategic communication to the Australian community about the regulatory scheme's purpose and safeguards (including prohibition on single identifier and in-built consent requirements). The Program's ongoing consultation process and transparency about decisions, their impacts and implementation will not cease with the passage of legislation.	Minor	**Finance (Legislation and Communication Functions)** – Throughout implementation, Finance will continue to manage the risks of public misunderstanding through multi-channel engagement (including in-person, through social media, and the Digital ID website). The website will continue to serve as a user-friendly, authoritative source of truth on the Digital ID System and its regulation, and will be maintained during and post-implementation. Public, industry, community and user sentiment will continue to be monitored through feedback received via these channels and engagement approaches tailored accordingly. Successful risk management also requires other stakeholders (**businesses, individuals and community)** to engage with these channels and continue participation in Government communication forums (both informal / ad hoc and formal structured forums – such as statutory advisory committees).

Challenge/risk	Likelihood	Consequence	Management	Residual risk rating	Relevant stakeholder(s) and roles / responsibilities
• **The compliance/ enforcement/ governance aspects of Option 3 may significantly impact other Government entities, including unintended consequences.**	Likely	Major	Whilst Finance is ultimately responsible for design and delivery, the Program adopted an agency partnership model from commencement, drawing on senior executives within partner agencies to seek alignment and agreement on the priorities and vision. This approach continues, 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.	Minor	**Finance** - ultimately accountable for the governance, strategy, policy, and administration of the system. **ATO, Services Australia**, and **The Attorney-Generals Department** – responsible for the delivery and operation of key government components of the system, including myGovID, the Digital Identity exchange, Document Verification Service and Face Verification Service. Senior executives will engage with Finance on governance and delivery matters, ensure alignment across implementation priorities and delivery. **Information Commissioner –** Has regulatory functions in relation to additional privacy protections in the Bill including biometric safeguard and limits on data profiling. Close engagement with Finance and OA will continue through implementation to operationalise these functions.

Challenge/risk	Likelihood	Consequence	Management	Residual risk rating	Relevant stakeholder(s) and roles / responsibilities
• **There are divergent views on Digital ID and the nature/scope of proposed regulation, meaning not all stakeholders will be satisfied with the final positions taken.**	Likely	Major	It is acknowledged that the Bill is unlikely to be acceptable to all stakeholders. At every stage, the Program has been fully transparent with stakeholders on its policy positions and reasoning and has amended many positions as a direct result of stakeholder feedback. Whilst not all stakeholders may be satisfied with the final position, the impact of this can be mitigated by continuing to demonstrate transparency regarding decision-making, and a genuine willingness to consult. Additionally, as set out in Section 10 Consultation above, consultation does not cease when the regulatory scheme commences, with stakeholders still able to inform future development of the regulatory framework.	Moderate	**Finance (Legislation, Communications and Engagement Functions)** – Throughout implementation, Finance will manage ongoing engagement on operationalisation of the regulatory scheme and will continue to display transparency regarding feedback received and reasons for final policy decisions taken. This is a continuation of the Program's existing consultation approach (which has entailed multiple rounds of public consultation, with outcomes of consultation published on the Digital ID website). Successful risk management also requires other stakeholders (**businesses, individuals and community)** to engage with these channels, take opportunities to understand the reasons for certain policy decisions, and continue participation in Government communication forums (both informal / ad hoc and formal structured forums – such as statutory advisory boards).

Challenge/risk	Likelihood	Consequence	Management	Residual risk rating	Relevant stakeholder(s) and roles / responsibilities
• **Even after the regulatory scheme commences, some detail may not be available due to the ongoing development of supplementary legislative instruments, rules and policies.**	Possible	Major	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 needs to evolve over time) is set out in supplementary instruments and artefacts. This means the regulatory scheme at the point of commencement may not contain all details impacting Digital ID 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. This is mitigated by the Bill including two sets of rules (both released 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 before introducing any change.	Minor	**Finance (Legislation, Policy and Strategy Functions)** – As the agency accountable for governance, strategy, policy and administration of the Digital Id System, Finance will continue to manage the development of further details related to the regulatory regime through implementation. It will use the established consultation, policy development and communication approaches that have been developed and deployed not just in recent regulation-specific consultation rounds, but on TDIF consultations over the past 4-5 years of the Program. Successful risk management also requires other stakeholders (**businesses, individuals and community)** to continue to take opportunities to participate in these ongoing consultations on future regulation, the TDIF and other matters. This includes continued participation in Government communication forums (both informal / ad hoc and formal structured forums – such as statutory advisory boards).

Challenge/risk	Likelihood	Consequence	Management	Residual risk rating	Relevant stakeholder(s) and roles / responsibilities
• **Management of dependencies such as the Australian Government's ongoing Privacy Act review.**	Possible	Major	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.	Minor	**Finance (Legislation, Policy and Strategy Functions)** – continue engagement and monitoring of the impact of other related Government initiatives (including the Privacy Act review) through the implementation period. Use established cross-Government forums and channels to raise any concerns or unintended impacts on the Digital ID regulatory scheme directly with AGD.

Table 9: Challenges and risks of implementation of Option 3

Whilst the above accurately describes the status of implementation risks as at the date of finalisation of this Impact Analysis, it is important to note that the Program has a dynamic risk management framework in place which is continuously evolving as planning progresses and the future state evolves, and if Government decides to roll out additional phases of its policy. Appropriate adjustments to the management activities, roles and accountabilities will continue to be made through the implementation period of this regulatory scheme. Risk management and other implementation activities will be regularly reviewed, including a formal legislative post-implementation review 2 years following the commencement of the Bill. This ongoing monitoring is discussed further below.

12.3 Ongoing monitoring of implementation effectiveness

Various measures built into the Bill provide for regular monitoring of the implementation of a dedicated regulatory scheme, and its ongoing effectiveness. These include:

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

Additionally, as discussed above, the legislation includes mandated consultation on proposed changes to regulations, 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 conclusion of any formal transition or implementation period.

Appendix A – Glossary

This glossary highlights key terms, acronyms, and their definitions, as used in this document.

Term	Definition
Access Card initiative	The Australian Government provided details of a health and social services Access Card in the 2006–07 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)	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	Registered on 27 October 2017 and commenced on 1 July 2018. The Code applies to all Australian Government agencies subject to the Privacy Act (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 Privacy Principles (APPs)	The cornerstone of the privacy protection framework in the Privacy Act. 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, biometric information is considered as sensitive information, which provides additional obligations on organisations.)
Council of Australian Governments (COAG)	The peak intergovernmental forum in Australia. It initiates, develops and monitors policy reforms of national significance which require co-operative action by Australian governments.

Term	Definition
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)	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 ID	Unless otherwise stated*, 'digital ID' (non-capitalised term) as used in this document may refer to: • an individual's digital ID – 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 ID; and/or • general/existing digital ID systems, activities and services (not specific to the Australian Government Digital ID System). *Not to be confused with other usages in this document – i.e. "Digital ID System" (see below), or the proposed legislative definition of "digital ID" (described in Section 5.3).
Digital ID Program (Program)	Delivered by Finance, in partnership with other government entities, it will, over time, allow individuals and government services to do more 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 ID that can be used to access online government services.
Digital ID System (System)	Generally, 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 ID System, as delivered by the Program and proposed to be regulated through the exposure draft Bill and rules, as distinct from other digital ID systems.
Digital Transformation Agency (DTA)	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)	Sets the direction for the DTA's work from 2018–25. 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 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 Digital ID Systems.

Term	Definition
Financial System Inquiry Report (Murray inquiry)	Released on 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 10–20 years characterised by the fair treatment of individuals. The Inquiry made 44 recommendations relating to the Australian financial system.
Government Business Enterprises (GBE)	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 standard that governs the security of government ICT Systems, produced by the Australian Signals Directorate (ASD). It comprises three documents targeting different levels: 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 body currently regulating the Digital ID 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, JobSeeker 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 require 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.

Term	Definition
New Payments Platform (NPP)	Launched in February 2018, it 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)	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)	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)	Produces independent analysis and statistics to promote policies to improve economic and social wellbeing across the globe.
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)**	Promotes and protects the privacy of individuals and regulates how Australian Government entities and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information. It includes 13 Australian Privacy Principles (APPs), which apply to some private sector organisations, as well as most Australian Government entities.
Privacy Impact Assessment (PIA)	Assessment that identifies the impact that a project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.
Private sector	The part of the economy that is run by individuals and companies for profit and is not state controlled. For the purposes of this Impact Analysis, it encompasses all for-profit businesses that are not owned or operated by the government.
Regulatory Technology (RegTech)	Management of regulatory processes in the financial industry through technology. Its main functions include regulatory monitoring, reporting and compliance.
Trusted Digital Identity Framework (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)	International NGO founded in 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 Digital ID System

Table 8 provides a more detailed description of the specific interactions and likely incentives of each type of entity currently involved in the Digital ID System, as described and depicted in Section 2.3.3 Entities, interactions and incentives within the current Digital ID System.

Entity type	Role, interactions and incentives within current Digital ID 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 ID 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, 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. One non-Australian Government IDPs (Australia Post's Digital iD) have been accredited but are not onboarded and available for individuals to select. Interactions: IDPs are the key contact point between the 'external' and 'internal' components. They interact directly with people through the creation of Digital IDs, 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 arrangements are 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 ID because this will support expanded adoption and use, justifying investment to date. At present there is no legislative mechanism by which IDPs can recover costs or charge other Digital ID System participants for their services within the TDIF.	myGovID Australia Post's Digital iD (accredited but not on-boarded and available as an IDP choice)

Entity type	Role, interactions and incentives within current Digital ID System	Example participants
	While it is theoretically possible for non-government entities to become IDPs, in practice there are limited incentives to 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 Australian Taxation Office's (ATO) 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 Digital ID System arrangements, APs are exclusively Australian Government agencies such as the ATO. These entities are resourced to participate in the Digital ID System because their involvement supports the ongoing expansion of Digital ID by diversifying the range of possible use cases.	ATO Relationship Authorisation Manager (RAM) MyGov (currently undergoing accreditation process)
Credential service provider (CSP)	Role: support the safety and security of the Digital ID 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). 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	myGovID Australia Post's Digital iD (accredited but not on-boarded and available in the Digital ID System as a CSP choice)

Entity type	Role, interactions and incentives within current Digital ID System	Example participants
	authenticate themselves when establishing a Digital ID or authorising verification by a relying party. 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 Digital ID 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 Digital ID System, managing interactions between all onboarded accredited entities operating within the TDIF . Incentives: The IDX is a crucial Digital ID 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 Digital ID 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* Digital ID 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	Various, including: Centrelink ATO State and territory revenue agencies (currently being tested under pilot conditions)

Entity type	Role, interactions and incentives within current Digital ID System	Example participants
	Digital ID, along with individuals. Participation in the Digital ID System is fully voluntary for relying parties. Interactions: Relying parties interact exclusively with IDXs. Incentives: Under current Digital ID System arrangements, only government entities can legally become relying parties. Entities have a strong incentive to do so because the use of Digital ID 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 Digital ID System, including ensuring the TDIF requirements are met by all onboarded accredited entities. The Interim Oversight Authority's functions are currently shared by Finance 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 Digital ID System. It then provides ongoing oversight of how entities behave within the Digital ID 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 Digital ID 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 Digital ID 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 Digital ID System.	Finance and Services Australia
User	Role: establish and use a Digital ID – 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	Individual citizens in private capacity Individuals in capacity as business owners

Entity type	Role, interactions and incentives within current Digital ID System	Example participants
	match the password for the account held by Jane Doe?'. Participation in the Digital ID 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 ID (along with relying parties) individuals interact exclusively with IDPs. They establish a Digital ID presence with an IDP 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 Digital ID System and would do so if it were not in place. Incentives: Users have a range of incentives to participate in the Digital ID 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 Digital ID System. However, it should be noted that several factors 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 ID outside of interaction with Australian Government entities.	

Table 10: Details of entities, interactions and incentives within the current Digital ID System

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

Table 9 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 Digital ID System, as described and visually depicted in Section 2.5.2 Entities, interactions and incentives within an expanded .

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 scenario 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 will remain the same. This is intended to ensure competitive neutrality between government IDPs and other participants. Incentives: An expansion will pave the way for a significantly larger number of organisations and individuals to participate, 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 ID 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 ID, creating a self-reinforcing loop of more relying parties generating more individual	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
	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 where there is an opportunity for them to gain financially from doing so. The Australian Government has acknowledged this and initiated design work on an appropriate charging regime 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 where charging arrangements do not impose unreasonably high costs, or where such costs can be recouped through other 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 expansion scenario, 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 will remain the same. Incentives: As with IDPs, under an expansion scenario it would be possible for APs to	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
	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 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. Where entities already deal with such 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 creates the opportunity for entities to participate as standalone CSPs, rather than this function being combined with that of an IDP. Incentives: The expansion 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.

Entity type	Potential role, interactions and incentives in an expanded System	Example participants
Relying parties		
Non-Australian Government relying party	Role: As in 'Current' table above. A key feature of an expansion scenario is the capacity for entities beyond the Australian Government to become relying parties. However, participation as a relying party would remain entirely voluntary. Interactions: As in 'Current' table above. Under an expansion scenario, 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: • 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 • 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 expansion scenario. 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 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 expansion scenario, it is anticipated that participation by private sector relying parties will be influenced to a greater degree by	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
	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 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. However, unlike the status quo, it would be expected that a governance body may have increased interaction with relying parties, particularly relating to any new charging framework 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. 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 an expansion scenario
User	Role: As in 'Current' table above. The role of users is expected to remain constant regardless of which IDPs they choose to use. Participation would remain fully voluntary. Interactions: Under an expansion scenario, 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 ID to verify themselves with a much wider range of relying parties, as non-government entities are enabled to join for the first time. Incentives: Expansion 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.	Individual citizens in private capacity Individuals in capacity as business owners

Entity type	Potential role, interactions and incentives in an expanded System	Example participants
	Expansion 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 ID outside of interaction with government entities. As direct charging of users is not anticipated within an expansion scenario, 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.	

Table 11: Details of potential entities, interactions and incentives in an expanded Digital ID System

Appendix D – Consultation Details

This Appendix provides further detail of consultation feedback considered by round of feedback or stakeholder segment, supplementing the discussion in Section 10 of the Impact Analysis. The below draws out broad themes for discussion and analysis purposes, however it is important to understand that the Program has received a significant quantity of diverse feedback over many years across a spectrum of stakeholders. Whilst best efforts have been made to accurately describe this feedback at a broad level, there are inherent limitations in generalising or attributing discrete sentiments or themes to what has consistently been very nuanced feedback on a complex issue.

Previous consultations

Table 15 below details the Program's schedule of consultations.

Consultation	Details	Timeframe occurred	No. of stakeholders engaged
PIAs	There have been multiple PIAs conducted on Digital ID, 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 Privacy and security | Digital Identity 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	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 ID Legislation Working Group (DILWG), a forum with representation from	Scoping Paper phase – March 2020 Draft Consultation phase – August 2020.	Scoping Paper phase – 23 Australian Government agencies Draft Consultation phase – 17 Australian Government agencies

Consultation	Details	Timeframe occurred	No. of stakeholders engaged
	thirteen 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 Australia. The DICJWG conducted four themed workshops inviting engagement in formulation of the three policy options.	Throughout 2020	8 states and territories in Australia Themed workshop invitations sent to all Australian jurisdictions
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 Digital ID System. Five webinars supported the release of the paper, 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

Consultation	Details	Timeframe occurred	No. of stakeholders engaged
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 sector groups, non-for-profit sector groups and various programs/status groups. Feedback was incorporated into the position paper.	Early months of 2021	23 submissions received
Targeted events with key industry and government associations	Following release of the position paper, targeted events with key industry and government associations occurred, 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
Targeted consultation with Australian Government agencies	Relevant Australian Government agencies were consulted once again for their input on the Bill prior to the release of the draft legislation as part of the Exposure Draft package. This occurred through multiple forums including the DILWG, the Steering and Portfolio Board, one-on-one consultations, and a webinar.	6 to 12 August 2021	• DILWG - 11 Australian Government agencies • Steering and Portfolio Board – 4 Australian Government agencies • 7 other Australian Government agencies

Consultation	Details	Timeframe occurred	No. of stakeholders engaged
Exposure draft package	The Program's most recent legislation-specific consultation saw the release of the exposure draft package. The package invited public views on the draft Bill, TDIF accreditation rules, TDI rules and (separately) Consultation RIS. Feedback received from previous consultation (including position papers) informed the draft Bill and supporting materials. In turn, the outcomes of consultation on the exposure draft have shaped the final policy positions taken in the Bill. The outcomes of consultation on the Consultation RIS validated and supported consideration of regulatory impacts and costs in the final Decision Impact Analysis.	1 to 27 October 2021	• 69 submissions received from industry and government stakeholders • Over 109,000 pieces of feedback, as well as over 6,200 emails, received from the Australian public, including individuals and small businesses
Targeted consultations on the *Transition and Consequential Provisions Bill* (T&C Bill)	Concurrent to the Program's exposure draft consultations, key Australian Government agencies were consulted on the T&C Bill, to support the transition of existing Digital ID System participants to the new Digital ID System (following implementation of the Bill).	One-on-one consultations – 14 to 21 October 2021 Briefings to the DILWG – 6 and 20 October 2021	• One-on-one consultations - 5 Australian Government agencies • Briefings to the DILWG - 11 Australian Government agencies

Table 12: Program's previous and relevant consultations held to ahead of October 2021 Exposure Draft

Consultation September-October 2023

Details	Date
Australian Information Industry Association (AIIA) Canberra Manager's Forum **AIIA Roundtable**	Tuesday 19 September
Targeted Bilateral discussions **Roundtable - Small Business Sector**	Wednesday 20 Sept
Digital Identity Working Group (State and Territory Governments)	Thursday 21 September
Public Webinar – Digital ID Legislation overview	Friday 22 September
Banking and Payments Sector Roundtable **FinTech / RegTech / Telcos roundtable**	Monday 25 September
Business Organisations Roundtable **Legal, Human Rights and Consumer Advocates Roundtable #1** **Inclusion Roundtable (Services Australia Advisory Groups)**	Tuesday 26 September
Bilateral – Privacy Commissioners Roundtable **Tech Council of Australia Roundtable**	Wednesday 27 September
Public Webinar – Deep Dive and Q&As **Inclusion Roundtable**	Thursday 28 September
Legal, Human Rights and Consumer Advocates Roundtable #2 **Reserved for additional requested meetings (ANZ)** **Youth Steering Committee** **Insurance, Retail, HR and Real Estate Roundtable**	Tuesday 3 October
State and Territory Chief Information Officers	Wednesday 4 October

Privacy Advocate Bilaterals	

Details October 2021 Public Consultation Round

The Table below details the key themes and issues drawn from the Program's earlier exposure draft package public consultation that occurred over October 2021.

Key finding / theme	Details of response	Impact on Program activity
Regulatory costs understated	Whilst most RIS submissions agreed that the impacts of Options 1 and 2 were accurately described, the view was expressed that Option 3 regulatory costs were under-stated, particularly for large entities operating across multiple lines of business.	The estimated regulatory costs for Option 3 were re-visited, with increased resource burden and a higher contingency applied to certain activities to account for additional variables raised by respondents to the Consultation RIS.
Scope of the Bill	Stakeholders raised questions on various definitions in the Bill, requested clarification on the extent of the Bill's powers in specific situations and queried whether the Bill may inadvertently regulate entities or services not intended to be regulated from a policy perspective.	Dialogue between the Program and the public has been revisited and strengthened, to provide further information and guidance clarifying the extent of the Bill's powers, the voluntary nature of participation and alignment with other regulatory schemes (re-iterating that the Bill leverages overarching principles from various existing definitions and regimes).
Complexity of the Bill	Some responses raised concerns around the inherent complexity of having two regulatory schemes (one around accreditation and the other around Digital ID System participation), as opposed to one combined scheme. These submissions queried on the effect this may have on public trust and understanding in the Digital ID System.	Dialogue between the Program and the public has been revisited and strengthened, to provide further information and guidance around the two schemes under the Bill and their respective purposes. In particular, education on the two regulatory schemes will form a core component of the implementation plan for the Program moving forwards. The Program has specifically designed

Key finding / theme	Details of response	Impact on Program activity
		the Bill to enable private sector participants different options for involvement with appropriately tailored regulatory requirements – in direct response to earlier feedback provided by the private sector in particular.
Governance	Feedback received included queries about the opportunities available for industry and cross-government (including state, territory and cross-jurisdictional) involvement in the Digital ID System's proposed governance arrangements. Some stakeholders also provided feedback on the Minister's power to make decisions with respect to the Rules, without the requirement of prior consultation.	Since the beginning of consultation, the Program has ensured that industry and Australian Government representatives have had an active platform to voice opinions and perspectives. The Program has established advisory committees to enable these stakeholders to support the OA in governance of the Digital ID System, and the Minister's ability to establish advisory committees is now entrenched in the Bill. The Program has also been continuously engaging with stakeholders on the issue of the scope of the Minister's powers to make decisions, and has directly addressed questions around what issues fall within and outside this scope. Overall, the Program has moved towards limiting the number of instances where the Minister is enabled absolute decision-making power in the legislation to narrow circumstances, for example national security reasons leveraging existing regulatory models and definitions. An example of a stakeholder response acknowledging the Program's active efforts in ensuring final policy positions related to governance issues reflect views expressed through ongoing consultation follows: *We appreciate the efforts made by the [Australian Government] to respond to the concerns raised by many stakeholders*

Key finding / theme	Details of response	Impact on Program activity
		regarding the proposed amount of delegated legislation and rulemaking that was described in the first consultation paper. (Source: Access Now input to Australia Digital ID Position Paper for proposed Trusted Digital Identity Bill (July 2021) (digitalidentity.gov.au))
Law enforcement access	Submissions saw divergent views on this issue, with some entities opposed to any form of law enforcement access, and others believing the current framework should be extended to allow for more access. Law enforcement agencies that responded voiced queries around how their current operations may be affected by the Bill.	The final policy positions on this issue, as reflected in the Bill, seek to achieve a balance between providing access to law enforcement in narrow, clearly defined circumstances, and recognizing the importance of restricting the use of particularly sensitive information, in order to achieve the goal of a citizen-centric system (for example, the legislation specifically prohibits disclosure of biometric information to law enforcement).
Charging	Most submissions received supported the idea that Australian citizens will not have to pay to participate in the Digital ID System. However, views were voiced around requiring further clarity on the details of the charging framework.	This feedback has informed the regulatory approach of including principles in the Bill that set broad parameters for the charging framework's operation (for example, ensuring legislative enshrinement of important principles such as the citizen not having to pay to participate), but leaving specific details to be determined through subordinate instruments. The Program's response effectively addresses the need for certainty as expressed through submissions, while also allowing for flexibility.

Details September-October 2023 Consultation Round

The Table below details the key themes and issues drawn from the Program's most recent exposure draft package public consultation that occurred across September and October 2023.

Key finding	Details of response	Impact on Program activity
There is strong support for Digital ID from business and industry	Business and industry support the rollout of Digital ID	Positive support from business and industry will assist the proposed Digital ID legislation. Increasing cyber breach events have emphasised the need for individuals transacting online to have a safe, secure and convenient way to prove who they are. Enshrining in legislation, privacy safeguards and enforceable penalties for breaches will build trust in the AGDIS and Accreditation Scheme.
Business wants to maximise inclusion and stronger branding	The Digital ID Taskforce is developing an Inclusion strategy which has a strong focus on accessibility, affordability and digital ability The passing of legislation will enable the development and use of a Trustmark for accredited services and AGDIS participants. The Trustmark will develop trust in the AGDIS and the Accreditation Scheme for providing a safe, secure option for transacting online.	The Digital ID Taskforce recognises that those that stand to benefit the most from a Digital ID will most likely be our most vulnerable members of society. The development of the Inclusion Strategy is underway and seeks to ensure that both the AGDIS and the Accreditation Scheme will provide best practice for various Inclusion aspects, but focussing on accessibility, affordability and digital ability. These policies will be developed with support from all levels of governments and privates sector input. Impact to the Taskforce is expected to be minimal.

Phasing and interoperability needs more consideration for private sector participation	The expansion of the AGDIS will be done in phases to ensure foundational elements of the AGDIS and Accreditation scheme are established before enabling private sector participation. Introduction of each phase will be a consideration for Government.	Phasing the expansion of the AGDIS is required to lay foundation components, specifically the establishment of Governance for the AGDIS, the associated roles and responsibilities and successful introduction of the draft legislation, enabling state and territory governments and private sector participation. The subsequent phasing will be enabled by Government where further consideration will be given to enabling private sector participation within the AGDIS.
Interoperability with other digital identity systems and digital wallets	The AGDIS has been built utilising a federated model allowing public and private sector identity providers to supply trusted digital identities to individuals and businesses. The federated model allows interoperability with the various developing digital identity ecosystems outside of the AGDIS. Policy development for digital wallets is underway	Earlier research focussed on the operation of digital ID systems across other international examples. This research led to inclusion of an interoperability obligation, clarifying the expectation of how entities would interact. There is zero to minimal impact expected to the program on the policy development for use of digital wallets.
Alignment with other Commonwealth reviews, legislative instruments and processes is required	The Taskforce are working across Commonwealth agencies to align developing legislation which seek to provide stronger cyber security protections and minimise duplication of regulatory requirements.	There is a potential impact pending outcomes of the Privacy Review.

What will be the associated charging and costs with participation and accreditation be?	Government will not charge for accreditation and participation during the first two phases of expansion Users will not be charged for creating and using a Digital ID Accreditation and service provider charges are still being considered by Government	Finance will develop an approach for charging, which will include public consultation, for Government consideration ahead of implementation of phases where the private sector can join the Australian Government Digital ID System. Policy development and charging work to inform this process and future charging arrangements.

Strong support for: **Digital ID to remain voluntary for Government services; and** **Government services continue to provide non digital options for individuals who cannot, or choose not to obtain a Digital ID**	The Government's key policy decision is that creation and use of a Digital ID by an individual to access Government services for an individual within the AGDIS will be voluntary. Services can seek an exemption from the Regulator to this requirement, such that they can require use of a Digital ID to access the service. This voluntariness principle does not apply to services where an individual is acting on behalf of another entity in a professional or business capacity The voluntariness principle does not apply for services operating outside of the AGDIS, including services provided outside the AGDIS by an accredited Digital ID provider	Impacts of the Voluntariness rule will be monitored to ensure Inclusion standards are met within the AGDIS. Further consultation is proposed through the Parliamentary process before legislation is passed. The Voluntariness principle may be reviewed again at the two year Review point and may also consider potential impacts of Voluntariness in the private sector.

Evolution of stakeholder views throughout consultation

The table below provides an overview of how the views of individuals, businesses, communities and governments on the Program and its regulation have evolved throughout consultation.

Stakeholder group	Initial views / positions on Program	Evolution of views and Program over consultation	Final views / positions on preferred Option
Individuals	• Generally indicated tentative positivity about Digital ID and its potential benefit • Expressed hesitation on matters including privacy, safety, security and other consumer impacts • Governance was raised as a substantial issue, with Governments having too much power being a concern. • Law enforcement access to Digital ID data was cited as a concern.	• Over time, informed the Program's regulatory approach of including more detailed, rather than lesser, safeguards and protections in the Bill • Airing of certain concerns from individuals led to certain safeguards being built into legislation, rather than being delegated to subordinate instruments – such as a legislative guarantee of the system's voluntariness.	Informed individual stakeholders continue to indicate tentative positivity towards the Digital ID System and regulation under Option 3. The Program has actively addressed concerns raised throughout consultation and reflected changes in the Bill. The Program continues to consult with this group through communication and education pieces to support their understanding. Governance concerns have been addressed through a new regulatory approach with the ACCC as initial regulator, and the Data Standards Chair being contained in the legislation. Changes Law enforcement access

Stakeholder group	Initial views / positions on Program	Evolution of views and Program over consultation	Final views / positions on preferred Option
			to Digital ID data has been changed in the legislation to achieve balance between security, safety, reducing fraud, and privacy concerns.
Businesses	1. Broadly supportive of a whole-of-economy Digital ID System 2. Sought clarity on the scope and application Digital ID 3. Queries around interoperability with other existing (current and future) systems	4. Dialogue between the Program and the business community, particularly those in relatively highly regulated sectors such as financial services and telecommunications, focused on alignment with other existing regulatory schemes in areas including privacy, anti-money laundering 5. Communication from the Program focused on explaining the legislative entrenchment of two distinct ways to be involved (accreditation and system participation), and the flexibility this allows for businesses specifically 6. Feedback from business' emphasized the need for certainty yet flexibility, which informed the inclusion of principles in the Bill setting broad parameters for the framework's operation, while leaving specific details to be determined through subordinate instruments	Businesses continue to be broadly supportive of regulation of an expansion scenario under Option 3. Many private sector entities see the Bill and the Program as a fundamental enabler of Australia's digital economy and have expressed interest in future participation (whilst emphasizing the importance of charging framework details to their ultimate decision to participate). The Program has actively consulted with this stakeholder group through public and targeted forums, and have adjusted several policy positions in response to feedback. The Program continues to consult with this group through communication and education pieces to

Stakeholder group	Initial views / positions on Program	Evolution of views and Program over consultation	Final views / positions on preferred Option
			support their understanding.
Government	7. Broadly supportive of a whole-of-economy Digital ID System 8. Raised concerns around the alignment with existing regulatory regimes, particularly State and Territory privacy authorities 9. Queries around the extent to which law enforcement agencies can access and use information within the Digital ID System	10. Supportive of modifications to contain appropriate exemptions for state / territory entities already meeting a similar level of privacy protection to Commonwealth privacy standards 11. Opinions from government led to revised policy positions seeking to achieve a balance between providing access to law enforcement in narrow, clearly defined circumstances, and recognizing the importance of restricting the use of particularly sensitive information	As early adopters of the System, government agencies have been broadly supportive of the Digital ID System for the longest period. Key agencies have been continuously consulted with since the Program's commencement. This stakeholder group has not shown opposition to regulation of the Digital ID System under Option 3. Concerns raised by government stakeholders, e.g. regarding alignment of regulatory regimes and law enforcement agencies, have resulted in revisions to policy positions and the Bill. The Program plans to continue to consult with this group, especially throughout its implementation plan.
Community	• Concerns raised regarding the practicalities of enforcing this	• The Program continues to liaise closely with the Australian Human Rights Commission (AHRC), the National Children Commissioner, and the	While community stakeholders are broadly supportive of Option 3 as the preferred option, the Program continues

Stakeholder group	Initial views / positions on Program	Evolution of views and Program over consultation	Final views / positions on preferred Option
	voluntary mandate	Attorney-General's Department in order to address concerns	to liaise with these stakeholders to address voiced concerns. This was a key theme raised in the consultation process in 2023.

Table 13: Evolution of stakeholder views on the Program over consultation

Appendix E – Regulatory costs: Methodology and assumptions

This Appendix outlines the approach taken to estimate net regulatory burden in the Impact Analysis. The Impact Analysis provides economy-wide, annualised regulatory burden estimates for each relevant Option, in accordance with the Regulatory Burden Measurement Framework. These costs reflect data derived from multiple data sources, including internal Australian Government analysis and external research, validated through direct consultation with potentially impacted entities through the Consultation RIS.

Methodology

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

- Identifying activities that would influence regulatory costs of a regulated entity under the relevant Option as either application, privacy and security obligation, ongoing obligation or administrative.
- Categorising the frequency of the activity as either start-up (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).
- For post start-up ad hoc activities, making assumptions on the expected annual frequency of each activity. These assumptions were informed by Government's experience working to date, internally tested and validated through public consultation.
- Estimating the resource effort (time taken) to comply with that requirement, taking the average-level scenario for each activity (see Assumptions below).
- Estimating labour costs associated with a regulatory task, by multiplying time taken to complete the required compliance activity (average-level scenario) by expected annual frequency of each activity and by hourly cost for relevant staff.
- This provides the annual cost of complying with the regulatory requirements for each activity per Option and entity group as relevant, and produces a yearly per-entity regulatory cost.

- Validating yearly per-entity regulatory costs through broad consultation with potentially impacted entities through the Consultation RIS, and adjusting data estimations and assumptions in accordance with responses received.
- Multiplying each yearly per-entity regulatory cost by expected economy-wide uptake rate (see Assumptions) for the entity group. This was calculated over the default 10 years of regulation considered by the Regulatory Burden Measurement Framework.
- Dividing the sum of all yearly, economy-wide costs for each entity group over the 10 years (per Option) by 10, to derive average annualised regulatory burden for each Option.

Note – the above approach was followed for all entity groups for Option 3.
As Option 2 involves fewer regulatory measures than Option 3 (mainly privacy-related), this was costed for GBEs by focusing on relevant privacy activities required by the legislation. Option 2 calculations have assumed that all 9 GBEs currently in existence in Australia would gradually seek to participate over the 10-year duration of regulation calculated (per the Regulatory Burden Measurement Framework). Option 2 does not distinguish between start-up and ongoing costs, because there are limited 'initial' regulatory requirements involved.

Assumptions and sources

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

- **Start-up or ongoing costs** – these classifications were derived from analysis of the nature of the regulatory activities prescribed to businesses, and further broken down per individual regulated entity for each considered Option. Start-up costs (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 ongoing costs (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). Ongoing costs maintained constant prices and were not inflated to take account of inflation over the

default 10-year duration of regulation calculated (per the Regulatory Burden Measurement Framework). These assumptions have been internally tested and were further validated through the public consultation process.

- **Year on year uptake** – based on internal Digital ID use case demand modelling, estimating the rate of potential uptake and adoption on an economy-wide basis over the next 10 years. Uptake estimates were based on publicly available data sourced through desktop research and a range of assumptions where no reliable data could be sourced (for example, the number of onboarded accredited participants was limited based on the assumptions of the total number of participating entities that would be commercially viable to support. From that saturation point, all further onboardings would only be as accredited entities).

  Year on year uptake included a yearly estimate of newly participating entities and of entities seeking to continue participation. Standard uptake rates, without yearly uplifts, were applied across Year 1 estimates (2022–23) though to Year 10 (2031–32).

  As a proportion of the total year on year uptake rate, the percentage of entities estimated to apply for and (separately) be approved for restricted attributes (incurring greater application and privacy and security obligations) was assumed to be 90% and 60% respectively. The percentage of entities (excluding the relying party entity group) estimated to be approved for IP3 (similarly incurring greater privacy and security obligations) was assumed to be 100% of the entities applying for restricted attributes. These assumed proportions were applied to the yearly per-entity regulatory costs of each entity group under Option 3, allowing for further nuance in the economy-wide figures derived.

- **Resource efforts** – estimated based on analysis of regulatory activities prescribed per individual regulated entity (within the 'business' sector) for each considered Option. This analysis was informed by Government's current understanding of the potential future regulatory activities, as detailed in the Bill (and where activities were considered within the scope of the Regulatory Burden Measurement Framework).

  To accommodate variations across size and maturity levels of potentially impacted private business entities when deriving resource effort estimations, a

'maturity spectrum' applying three ranging resource effort scenarios was used to cost regulatory activities. The scenarios underpinning the maturity spectrum were drawn from experiences shared by a range of entities encountered through internal and external consultation. These consultation sessions revealed that entities and their facilities needed to meet, at a minimum, a 'baseline' level of maturity (outside of the regulatory requirements) to seek entry into the digital ID market. Accordingly, all scenarios within the maturity spectrum assumed entities met, at a minimum, this baseline level required for market entry. The estimated resource efforts required by low maturity entities were not considered within the maturity spectrum, as these entities were considered still premature for market entry.

The scenarios considered within the maturity spectrum included:

- **Low-level scenario** – estimating resource effort required by a *high maturity entity,* usually with established technical systems/processes, mature privacy and security arrangements and available experienced resources
- **High-level scenario** – estimating resource effort required by a *medium maturity entity** meeting the minimum facility and resource thresholds of accreditation, usually with less established technical systems / processes, few privacy & security arrangements and few available experienced resources
- **Average-level scenario** – average of the low-level and high-level resource effort calculations.

*The minimum entity maturity considered by the maturity spectrum was a medium maturity entity (within high-level scenario). The maturity spectrum assumed that low maturity entities did not, at a minimum, meet the 'baseline' level of maturity required for entry into the digital ID market, and thus their corresponding estimated resource efforts were excluded from calculations.

- **Contingency costs** – Included as an approximate 10% flat rate allocation within the three resource impost scenarios (low, average and high).
- **Labour rates** – In accordance with Australian Government guidance, the default hourly labour rate contained in the Regulatory Burden Measurement Framework was used. This was based on average weekly earnings, adjusted to

include income tax. This provided an economy-wide value for employees of $41.74 per hour. This value was then scaled up using a multiplier of 1.75 (or 75 per cent as per the Regulatory Burden Measure) to account for 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 resulted 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 where regulation cuts across a number of sectors, as is the case for regulation. Note: 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.

- **Technology and System uplifts** – Regulatory burden estimates produced by the methodology described above are based on the most relevant information available at time of calculation. They are subject to change based on potential future technological uplifts to existing systems and enabling infrastructure facilitating participation in the Australian Government Digital ID ecosystem.
- **General** – This Impact Analysis over-estimates, rather than under-estimates, potential regulatory costs. This has been a guiding principle through this costing, including in making assumptions. For example, it has been assumed that all entities applying for initial accreditation will seek to maintain accreditation, incurring corresponding re-accreditation regulatory burdens, over the 10-year default duration of the regulation (per the Regulatory Burden Measurement Framework). This may not be the case once regulation is in place.

  Only regulatory measures which necessitated some positive action from regulated entities were included within calculations (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) were not included, being planned to be enabled by design and not requiring positive activity by regulated entities. Many regulatory requirements included provision for exemptions based upon defined criteria, however to ensure completeness for regulatory costing purposes it was assumed that exemptions would not be granted.

Detailed Calculations

This section includes detailed calculations that underpin the RBE tables included in Section 8.2 and Section 9.2.2 of the RIS.

Option 2

As described in the methodology above, Option 2 involves fewer regulatory measures than Option 3 (mainly privacy-related) and was costed for GBEs by focusing on relevant privacy and security obligation activities required by the legislation. In calculating Option 2 regulatory costs, relevant privacy and security obligation activities were identified from the legislation and assumptions around the expected resource effort required (time taken) and annual frequency of each activity (per the methodology and assumptions described above) were validated with stakeholders. Option 2 does not distinguish between start-up and ongoing costs, because there are no 'initial' regulatory requirements involved. Table 11 below shows the per annum cost,10-year average with a 10% contingency incorporated (see assumptions).

The annual costs were calculated as follows:

estimated time taken (average-level scenario) x *expected annual frequency* x *estimated labour cost* ($73.05 per hour) = *annual regulatory cost*

Noting that the expected annual frequency is based on the number of entities expected to be undertaking the activity and the frequency that the activity would be required to be undertaken each year by these entities. The assumptions regarding onboarding of entities can be found in Table 12 below. It is assumed that all nine GBEs in existence in Australia would gradually seek to participate over the first four years of regulation calculated.

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10	Total	10-year average		Contingency applied
Relying party (non-government)														
Privacy & Security Obligations	$9,039.32	$15,065.53	$21,091.74	$27,117.96	$27,117.96	$27,117.96	$27,117.96	$27,117.96	$27,117.96	$27,117.96	$235,022.29	$23,502.23		$2,136.57
Accredited entity (non-government)														
Privacy & Security Obligations	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00		$0.00
Onboarded accredited entity (non-government)														
Privacy & Security Obligations	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00		$0.00

Table 14: Option 2 estimated per-entity annual regulatory costs across 10-years of regulation (per the Regulatory Burden Measurement Framework)

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10
New GBE relying parties	**2**	**2**	**2**	**2**	**0**	**0**	**0**	**0**	**0**	**0**
Ongoing GBE relying parties	**3**	**5**	**7**	**9**	**9**	**9**	**9**	**9**	**9**	**9**

Table 15: Option 2 expected year on year Digital ID System uptake of GBE relying parties

Option 3

Option 3 involves the most significant regulatory measures for the categories of regulated entities, being relying parties, accredited entities and onboarded accredited entities. The regulatory impacts of Option 3 fall into the broader groups of application-related activities, privacy and security obligations, ongoing obligations and administrative activities required by the legislation (see Section 9.2 for further detail), which were validated through the Consultation RIS. In calculating Option 3 regulatory costs, relevant activities were identified from the legislation and grouped accordingly. Assumptions around the resource effort required (time taken) and annual frequency of each activity (per the methodology and assumptions described above) were drawn and further validated with stakeholders. Option 3 does distinguish between start-up and ongoing costs, with 'initial' regulatory requirements required, and these were accordingly considered as part of calculations. Table 13 below shows the per annum, 10-year average with a 10% contingency incorporated (see assumptions).

The annual costs were calculated as follows:

estimated time taken (average-level scenario) x *expected annual frequency* x *estimated labour cost* ($73.05 per hour) = *annual regulatory cost*

Noting that the expected annual frequency is based on the number of entities expected to be undertaking the activity and the frequency that the activity would be required to be undertaken each year by these entities. The assumptions regarding onboarding of entities can be found in Tables 14, 15 and 16 below. These assumptions have been based on internal Digital ID use case demand modelling, estimating the rate of potential uptake and adoption on an economy-wide basis over the next 10 years (per the Regulatory Burden Measurement Framework).

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10		10-year average		Contingency applied
											Total			
Relying Party (non-government)	**489,594**	**533,453**	**575,384**	**625,884**	**676,384**	**726,883**	**776,298**	**826,798**	**877,298**	**927,797**	**7,035,773**	**703,577**		**639,616**
Application	177,797	169,229	160,660	160,660	160,660	160,660	160,660	160,660	160,660	160,660	1,632,310	163,231		148,392
Privacy & Security Obligations	311,796	364,224	414,724	465,224	515,723	566,223	615,638	666,138	716,637	767,137	5,403,464	540,346		491,224
Ongoing Obligations	-	-	-	-	-	-	-	-	-	-	-	-		-
Administrative	212,551	248,548	282,830	317,113	351,395	385,678	419,960	454,243	488,525	522,807	3,683,650	368,365		334,877
Accredited Entity (non-government)	**268,689**	**345,824**	**260,975**	**327,183**	**446,743**	**511,023**	**575,302**	**639,582**	**703,862**	**768,141**	**4,847,325**	**484,732**		**440,666**
Application	165,841	165,841	55,280	82,921	138,201	138,201	138,201	138,201	138,201	138,201	1,299,091	129,909		118,099
Privacy & Security Obligations	-	-	-	-	-	-	-	-	-	-	-	-		-
Ongoing Obligations	102,847	179,983	205,695	244,262	308,542	372,822	437,101	501,381	565,660	629,940	3,548,234	354,823		322,567
Administrative	-	-	-	-	-	-	-	-	-	-	-	-		-
Accredited Participant (non-government)	**285,401**	**323,969**	**362,537**	**357,395**	**295,686**	**295,686**	**295,686**	**295,686**	**295,686**	**295,686**	**3,103,419**	**310,342**		**282,129**
Application	92,563	92,563	92,563	61,708	-	-	-	-	-	-	339,396	33,940		30,854
Privacy & Security Obligations	-	-	-	-	-	-	-	-	-	-	-	-		-
Ongoing Obligations	192,839	231,407	269,974	295,686	295,686	295,686	295,686	295,686	295,686	295,686	2,764,023	276,402		251,275
Administrative	-	-	-	-	-	-	-	-	-	-	-	-		-
Total regulatory cost for non-	**1,043,684**	**1,203,247**	**1,198,896**	**1,310,462**	**1,418,813**	**1,533,592**	**1,647,287**	**1,762,066**	**1,876,845**	**1,991,625**	**14,986,517**	**1,498,652**		**1,362,411**

government entities														
Application	436,201	427,633	308,504	305,290	298,862	298,862	298,862	298,862	298,862	298,862	3,270,797	327,080		297,345
Privacy & Security Obligations	311,796	364,224	414,724	465,224	515,723	566,223	615,638	666,138	716,637	767,137	5,403,464	540,346		491,224
Ongoing Obligations	295,686	411,389	475,669	539,949	604,228	668,508	732,787	797,067	861,347	925,626	6,312,257	631,226		573,842
Administrative	212,551	248,548	282,830	317,113	351,395	385,678	419,960	454,243	488,525	522,807	3,683,650	368,365		334,877

Table 16: Option 3 estimated per-entity annual regulatory costs across 10-years of regulation (per the Regulatory Burden Measurement Framework)

New relying parties	22	21	20	20	20	20	20	20	20	20		
Ongoing relying parties	124	145	165	185	205	225	245	265	285	305		
												Proportion*
Entities applying for restricted attributes	20	19	18	18	18	18	18	18	18	18		90%
Proportion of entities approved for restricted attributes	12	11	11	11	11	11	11	11	11	11		60%
Proportion of	12	11	11	11	11	11	11	11	11	11		100%

entities approved for IP3												

Table 17: Option 3 expected year on year Digital ID System uptake of relying parties

* Proportion (percentage) of new relying parties estimated to apply for and (separately) be approved for restricted attributes and IP3. These entities are expected to incur greater application and privacy and security obligations as a result.

New accredited entities	6	6	2	3	5	5	5	5	5	5		
Ongoing accredited entities	8	14	16	19	24	29	34	39	44	49		
												Proportion *
Entities applying for restricted attributes	5	5	2	3	5	5	5	5	5	5		90%
Proportion of entities approved for restricted attributes	3	3	1	2	3	3	3	3	3	3		60%
Proportion of entities approved for IP3	3	3	1	2	3	3	3	3	3	3		100%

Table 18: Option 3 expected year on year Digital ID System uptake of accredited entities

* Proportion (percentage) of new accredited entities estimated to apply for and (separately) be approved for restricted attributes and IP3. These entities are expected to incur greater application and privacy and security obligations as a result.

New onboarded accredited entities	**3**	**3**	**3**	**2**	**0**	**0**	**0**	**0**	**0**	**0**		
Ongoing onboarded accredited entities	15	18	21	23	23	23	23	23	23	23		
												Proportion *
Entities applying for Restricted Attributes (RA)	8	8	5	5	5	5	5	5	5	5		90%
Entities approved for Restricted Attributes	5	5	3	3	3	3	3	3	3	3		60%
Entities approved for IP3	5	5	3	3	3	3	3	3	3	3		100%

Table 19: Option 3 expected year on year system uptake for onboarded accredited entities

* Proportion (percentage) of new onboarded accredited entities estimated to apply for and (separately) be approved for restricted attributes and IP3. These entities are expected to incur greater application and privacy and security obligations as a result.

Appendix F – Figures and tables

A.1 Figures

A.2 Tables

Appendix G – Risk Matrix

The Risk Matrix used for assessing implementation risks (both untreated and residual) in Section 12 is set out below.

			Consequence				
			Insignificant	**Minimal**	**Medium**	**Major**	**Severe**
			A risk event that if it eventuates, the consequence will have little or no impact on achieving objectives.	A risk event that is it eventuates, the consequence will have a minor impact on achieving objectives, to the extent that one or more agreed outcomes will fall below expected but well above minimum acceptable levels.	A risk event that if it eventuates, the consequence will have a moderate impact on achieving objectives, to the extent that one or more agreed outcomes will fall below expected but above minimum acceptable levels.	A risk event that if it eventuates, the consequence will have a significant impact on achieving objectives, to the extent that one or more agreed outcomes will fall below acceptable levels.	A risk event that if it eventuates, the consequence will have a severe impact on achieving objectives, to the extent that one or more agreed outcomes are unlikely to be achieved.
Likelihood	**Almost certain**	Expected in most circumstances – 80% or greater possibility	Minor	Moderate	High	Very High	Very High
	Likely	Will probably occur in most circumstances – 50% to 80% probability	Low	Minor	Moderate	High	Very High
	Possible	Might occur at some time – 20% - 50% probability	Low	Minor	Moderate	High	High
	Unlikely	Could occur at some time – 5% to 20% probability	Low	Minor	Minor	Moderate	High
	Rare	May only occur in exceptional circumstances – less than 5% probability	Low	Low	Minor	Moderate	Moderate