Digital Identity Position Paper Consultation

Submission by the Australian Information Industry Association

About the AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. We are a not-for-profit organisation to benefit members, and AIIA membership fees are tax deductible. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity.

We do this by delivering outstanding member value by:

• providing a strong voice of influence

• building a sense of community through events and education

• enabling a network for collaboration and inspiration; and

• developing compelling content and relevant and interesting information.

We represent the end-to-end digital ecosystem in Australia, including:

• multinational companies

• large Australian technology, telecommunications and digital and cloud infrastructure companies; and

• a large number of small and medium businesses, start-ups, universities and digital incubators.

Cross-jurisdictional considerations and existing Digital Identity systems

Design of the DI framework needs to carefully consider cross-jurisdictional and business workflows operating in different settings. The utility and cross-jurisdictional value of an identity scheme should be paramount considerations in a federation.

The AIIA believes that a federated and cooperative co-design approach, especially with those arms of government that currently deal with current default identity in state drivers' licenses, including digital licenses and their undergirding data systems is important for cross-jurisdictional adoption and support. Explicit consideration should also be given as to how private identity systems are being utilised by large technology companies.

Privacy considerations and consumer preparedness

Government needs to ensure that the needs of the citizen are central not only to the end UX, but also that the trade-off or social compact between citizen and government is well considered and accepted. It is important that opt-in requirements do not require providers or consumers to trade convenience and improved experience for even a perceived erosion of privacy. Government needs to ask how the value of a national Digital Identity scheme can best be explained to its citizens, and in so doing must implement an ethical data trading framework that is both simple to access and of clear benefit to each citizen. Government needs to clearly articulate the benefits to the citizen of the DI so that barriers to adoption are lessened. One recommendation would be to link a major citizen service delivery

improvement that can only be utilised through acceptance and adoption of DI (e.g. through loading proof of identity verification in MyGov).

Proposed data model and interoperability

The proposed data model for the Digital Identity scheme needs to have interoperability with adjacent systems as a core requirement. As an example, the My Health Record systems have encountered core design challenges making it complex to operate alongside the next generation of digital systems, given MHR's centralised data model.

Provision of Use Cases

The government should consider providing some detailed use cases as part of an explanatory memorandum in conjunction with the draft Bill to increase the confidence levels of industry and individual participants in the Digital Identity system and its various applications. We note that the position paper provides a clear high-level framework for Digital Identity but remains somewhat vague in terms of detailed controls and use case examples, which may be useful to help prospective participants conceptualise how the Digital Identity system will operate in practice across a range of industries.

Enforcement and governance

The legislation will need to clearly delineate between the roles and responsibilities of the Oversight Authority and other agencies anticipated to have conferred functions under the legislation, such as the Information Commissioner, to avoid regulatory overlap issues. There may be scope for an incident such as a data breach that affects Digital Identity records to result in breaches of non-privacy and privacy-related provisions under the legislation that could engage multiple regulators on the Position Paper, which indicates that the Oversight Authority's role may include coordinating responses to security incidents, disaster recovery and other incidents that impact the system and provide redress for victims of identity crime, as well as issuing directions to Participants. However, it is proposed that the Information Commissioner will be responsible for monitoring and investigating breaches or suspected breaches of the additional privacy safeguards. This in itself creates much potential for overlap. The legislation needs to clarify how multiple agencies will collaborate in their response to events that have impacts spanning these areas of related responsibility, and be structured so as to minimise duplication of administrative effort by affected participants.

We note that the Bill will require Accredited Participants which are APP (**A**ustralian **P**rivacy **P**rinciples) entities to provide a copy of any data breach notice given to the Office of the Australian Information Commissioner (**OAIC**) under the Notifiable Data Breaches (**NDB**) scheme to the Oversight Authority as well, and in this respect it is proposed that the Bill will draw on the definitions and concepts in the Privacy Act's NDB scheme, including specifying what is a notifiable data breach for the system, when a breach has occurred or a suspected breach must be investigated, when remedial action has been taken, when the breach is to be notified to the Oversight Authority, and in what form. We understand it is proposed that the Bill will draw on the definition of "eligible data breach" and agree with this approach, and also suggest that, if a parallel notification system is introduced, operational aspects of the notification regime under the Bill (such as the notification form) be as closely aligned as possible with the NDB scheme under the Privacy Act for the sake of administrative efficiency.

Identity exchanges & restrictions on data profiling

- It is proposed that the legislation will prohibit Accredited Participants from collecting, using and disclosing information about a User's behaviour on the system however such information may be required to be used for various legitimate regulatory purposes, such as suspicious matter reporting. There is also a carve-out for responding to lawfully made requests for information for an enforcement purpose (subject to the prohibition on speculative profiling for an investigatory purpose), but currently the way this is drafted does not seem to include in its scope regulatory matters such as suspicious matter reporting.

- We understand that identity exchanges are in place to facilitate the private and secure sharing of digital identity information between participants in a digital identity system. Identity providers generate and manage the User's digital identity (i.e. verify User's identity and share verified digital identity with relying parties) while relying parties use the Digital Identities. For regulated entities under the Anti-Money Laundering (**AML**) regime to be able to rely on another entity engaging in Know Your Customer (**KYC**) there is generally a level of due diligence required, which might need to be covered by the rules of the exchange. Liability would also be an issue here, as discussed further in a below section.

Audit rights and reporting requirements

The financial services regulators (APRA and AUSTRAC) at times require rights of access to types of Digital Identity-related information, particularly where required for financial intelligence purposes. It is unclear how this access might practically take place given the proposed structure of the DI system. The government needs to consider whether a central information database would be established the ramifications thereof.

In addition to the reporting of data breaches, it is possible that there could also be duplication of reporting requirements for entities governed by the AML regime. For example, at 5.4.14, the Position Paper indicates that the Legislation would impose obligations on relying parties to notify the Oversight Authority of any security or fraud incident impacting the system and assist with resolution. This could conceivably overlap with reporting requirements under the AML regime, and perhaps could be adjusted to prevent duplication.

Privacy and consumer safeguards - building on existing laws, fostering participation and innovation

The AML regime requires that specific types of information be collected for the purposes of identifying or verifying different types of corporate structures. For the Digital Identity system to be useful for financial institutions and to foster participation in the scheme, the types of information collected for individuals could be better aligned with the type of information required to be collected for individuals under the AML regime, including "reliability" thresholds. Perhaps this should be considered as part of defining the TDIF accreditation terms. The "permitted purposes" for re-proofing may also need to be adjusted to better align with AML mechanisms.

Liability and redress:

Conceptually, the government should consider whether it is appropriate to have a statutory liability framework for working out how losses or damage suffered by individuals or entities using the system will be managed, as opposed to enabling participants to agree appropriate liability provisions via contract.

We can see arguments as to why a standard or systematic approach to liability may be necessary to encourage participation and confidence in the system and its rules, particularly in its early stages, but if a statutory liability framework is to be set out in the legislation, it is important for the principles of liability set out in the framework to be clear, and the legislation should clarify whether these statutory principles override any alternative liability provisions that may be agreed under contract between the Parties.

Incomplete or inaccurate details or discrepancies in identification and verification information are serious issues from an AML perspective and the regulator takes this seriously. Failures in this space could lead to significant penalties for regulated financial institutions relying on the Digital Identity system. The AIIA would query whether these possibilities have been considered under the proposed liability and redress framework.

On the issue of clarity and certainty of the proposed statutory liability principles, the Position Paper includes a number of references to relief from liability being available in circumstances where an entity is acting in good faith. For example, it proposes that, under the Legislation, an Accredited

Participant will not be liable for loss or damage suffered by a Participant using the system provided that the Accredited Participant was acting in good faith and in compliance with the legislative rules and requirements relating to the system. However, the reference to "good faith" may create legal uncertainty. If the test to qualify for relief from liability is to include an element of "acting in good faith", the concept of "good faith" must be clearly articulated under the Legislation.

It is proposed that the Oversight Authority or advisory boards would receive broad relief from liability except in cases of fraud, which is a high bar. The AIIA would query whether this this is appropriate particularly in relation to the Oversight Authority, considering it is responsible for accreditation and could cause loss to participants. This could create a perception that the government is not willing to stand behind its Digital Identity system and could reduce participants' confidence in the system, notwithstanding the fact that Oversight Authority decisions are to be subject to external merits review by the Administrative Appeals Tribunal.

Charging Model

While acknowledging that a charging model may be necessary and appropriate in principle to ensure the ongoing viability of the digital identity system, the proposed charging framework could present a barrier to entry particularly for smaller players, with a risk that the cost of participating may be too high for some players altogether, reducing participation rates.

While the proposed the Legislation will not impose charges on Users, we note that the proposed Legislation will not regulate fees charged by relying parties to an individual wanting to access its service(s) using the system. As a result, the system essentially imposes additional costs on relying parties that relying parties will either need to absorb as costs to the business that erode their margins, or ultimately pass on to end users as fees for access to their goods or services. Some service providers (particularly small providers) may not be in a competitive position to pass on such costs to their Users, leaving them out of pocket and therefore unlikely to participate in the regime.

The AIIA suggests that consideration should be given to a two-year moratorium on fees to encourage adoption of the scheme and ensure a sensical charging framework based on real-world use.

One option to ensure that the charging framework is feasible for small players to participate is to implement a tiered charging framework that takes into account usage so that smaller businesses can access digital identity services at a lower fee compared to larger businesses. Fees could also take into account the level of assurance required by the relying party, as well as volume. We note that these principles are, at a high level, reflected in Principle 4 of the Charging Principles and agree with this Principle, but feel that it may not go far enough to ensure that smaller parties feel they are supported to participate in the Digital Identity scheme.

Additionally, to foster participation in the Digital Identity scheme by such smaller parties that may otherwise not be able to absorb the cost of participating or pass on the cost to their Users, the legislation could provide for an exemption from the charging model for "small relying parties" or similar that meet a threshold linked to their annual turnover, number of employees, or a more specific metric relevant to their consumption of digital identity services like revenue per customer or transaction, to support SME participation.

For more information about the content of this submission, please contact policy@aiia.com.au.