Submission by the Australian Information Industry Association (AIIA) to the

Senate Economics Legislation Committee inquiry into the Digital ID Bill 2023 & Digital ID (Transitional and Consequential Provisions) Bill 2023

February 2024

Introduction

The AIIA thanks the Senate Standing Committee for Economics for the opportunity to respond to the inquiry into the Digital ID Bill 2023 (DI Bill) & Digital ID (Transitional and Consequential Provisions) Bill 2023. The Digital Identity Bill of 2023 and the Digital Identity (DI) scheme present an ambitious framework aimed at simultaneously modernising identity verification and minimising data collection in the digital economy to which the AIIA is a strong advocate and supporter.

The DI scheme is voluntary in nature and for the scheme to be a success and achieve widespread adoption, it must:

1. Maintain the trust of citizens;
2. Have strong privacy protections;
3. Have strong cyber security protections; and
4. Provide a benefit to the user or citizen by making the use of the scheme more efficient, easier or access new innovative services.

The scheme will fail if it loses citizen trust. The primary objective is to deliver seamless digital services and unlock productivity benefits across the economy. A micro example of this is the recent allowance of the Commonwealth digital ID (MyGov) to allow witnessing of commonwealth statutory declarations that will avoid the need to get a JP or police officer signature.

The AIIA notes that over 10 million Australians are already using the government's digital ID (MyGovID) so there is an excellent platform and trust in the digital identity tools, the challenge for government remains around that seamless customer and citizen experience and "front door" to government service delivery. Without ongoing investment by governments, the benefits will not be realised.

General Support for Digital Identity Bill

In line with its submission on October 2023,[1] the AIIA positively views and supports the Government's commitment to:

- Data minimisation and privacy (Chapter 3)
- data protection (ss 135-6);
- user experience, inclusion and accessibility (s 30);
- interoperability (s 79);
- consultations on Digital ID Data Standards (s 100) and Digital ID Rules (s169)

[1] AIIA, Submission on the 2023 Digital ID Draft Legislation (and Rules), October 2023.

Phased approach to implementation

The AIIA views the DI system as creating a secure and trusted framework that will result in innovation and entrepreneurialism from a wave of new services and offerings. This has happened in other economies following the establishing of digital ID and payments (e.g. India saw a 1.2% boost to their GDP as a result of the efficiencies and innovations allowed by their scheme). The interoperability requirement is an important pillar in the DI rules that supports a system that fosters competition and innovation.

Recommendation: The AIIA supports the scheme and would like to see the phased approach from phase one to four and the full economy adoption be compressed and accelerated so as to achieve the full economic benefits sooner. The multi-year approach and slow adoption could be considered a risk to its success and delay the innovation, productivity and service delivery improvements that will occur.

Section 49 privacy and law enforcement safeguards

As stated in the introduction, citizen trust is critical to the success of the scheme and the scheme is not a law enforcement tool. Any access to citizen provided personal information requested by law enforcement thus must meet a very high bar. The bill could include a more restrictive set of conditions as to what would constitute a justifiable reason for seeking a warrant. For example, terrorism, potential loss of life, kidnapping would be reasons to seek a warrant.

The narrow drafting on the disclosure of the accredited entity data by law enforcement is preferred as should future scenarios and law enforcement requirements be identified, amendments can be passed by the parliament. Cyber security laws present the case study where in recent years amendments are being passed annually or bi-annually (as is expected in 2024) to update laws following a policy review or breach of data. The same approach should apply to the DI scheme so that citizen trust is maintained on launch to ensure widespread adoption.

Digital ID Bill 2023 No. , 2023

Chapter 3 Privacy Part 2 Privacy Division 2 Additional privacy safeguards
Section 49 Authorised collection, use and disclosure of biometric information of individuals – general rules

(3) An accredited entity is authorised to disclose biometric information of an individual to a law enforcement agency (within the meaning 3 of the Australian Crime Commission Act 2002) only if:

(a) the disclosure of the information is required or authorised by or under a warrant issued under a law of the Commonwealth, a State or a Territory; or

(b) the information is disclosed with the express consent of the individual to whom the biometric information relates, or 9 purports to relate, and the disclosure is for the purpose of:

(i) verifying the identity of the individual; or

(ii) investigating or prosecuting an offence against a law of the Commonwealth, a State or a Territory.

Consultation on Cyber Security legislation and existing international standards

The AIIA notes that this Bill contains a definition of 'cyber security incident' in s 9, which is an important precursor for the determination of suspension (s 25) and revocation (s 26 or s 72) of accreditation. The Bill added but did not define the terms, 'unacceptable risk' and 'serious', as considerations for the Digital ID Regulator in suspending or revoking the accreditation.

Notwithstanding, the Department of Home Affairs is presently consulting on the introduction of a Cyber Security legislation, which will itself likely introduce a definition for cyber security incident.

Furthermore, the well-regarded European Union has a broader principle-based definition of cyber security incident in Directive (EU) 2016/1148.

Digital ID Bill 2023 No. , 2023

Part 2 – Interpretation
s 9 Definition

***cyber security incident** means one or more acts, events or circumstances that involve:*
(a) u4nauthorized access to, modification of or interference with a system, service or network; or
(b) an 4unauthorized attempt to gain access to, modify or interfere with a system, service or network; or
(c) u4nauthorized impairment of the availability, reliability, security or operation of a system, service or network; or
(d) an 4unauthorized attempt to impair the availability, reliability, security or operation of a system, service or network.

s 25 Suspension of accreditation
(3) The reference to cyber security incident in paragraph (2)(b) does not include acts, events or circumstances covered by paragraph (b) or (d) of the definition of that term unless the Digital ID Regulator is satisfied that the attempts referred to in those paragraphs involve an unacceptable risk to the provision of the entity's accredited services

s 26 Revocation of accreditation
(2) The Digital ID Regulator may, in writing, revoke an entity's accreditation if:
(a) the Digital ID Regulator reasonably believes that the accredited entity has contravened or is contravening this Act; or
(b) the Digital ID Regulator reasonably believes that:
(i) there has been a cyber security incident involving the entity; and
(ii) the cyber security incident is serious;

s 72 Revocation of approval to participate in the Australian Government Digital ID System
(2) The Digital ID Regulator may, in writing, revoke an approval given to an entity under section 62 if:
(a) the Digital ID Regulator reasonably believes that the entity has contravened or is contravening this Act; or
(b) the Digital ID Regulator reasonably believes that:
(i) there has been a cyber security incident involving the entity; and
(ii) the cyber security incident is serious; or…

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

*Article 4 **Definitions***

(7) 'incident' means any event having an actual adverse effect on the security of network and information systems;

The AIIA is also concerned that this DI scheme does not aligned with some existing data breach reporting obligations, such as under the Commonwealth Privacy Act (or state/territory equivalents) or security of critical infrastructure legislation. Consequently, accredited entities will have increased compliance burdens to manage different reporting obligations and timelines.

Recommendation: The AIIA suggests the Senate ensure references to cyber security in this Bill and the Digital ID Rules will be aligned with the legislative changes by the Department of Home Affairs. The AIIA also reiterates the importance of the Bill to be in line with international standards in its October 2023 submission, noting that a common definition will assist in guiding participating Multinational Corporations and international policing.

Recommendation: The AIIA notes that the lack of definition of 'unacceptable risk' or 'serious' will cause confusion and result in challenges by interested entities or parties. It is important that there is clarity and consistency in the interpretation of the Bill by affected parties. Due the interoperable nature, relying parties and individuals may lose their ability to access services if their chosen identity service provider is suddenly excluded.

Governance Structure

The AIIA is concerned that the DI scheme will be fragmented and plagued by inconsistencies, due to the multiple agencies and regulators involved.

Oversight and enforcement of the Digital ID laws will be shared between:

- ACCC as an independent Digital ID regulator;
- Services Australia as the "System Administrator" of the Australian Government Digital Identity System; and
- Australian Information Commissioner on privacy matters.

Recommendation: The AIIA acknowledges the importance of functional separation between the rulemaking (Minister), enforcement (Regulators) and operations (System administrator). Nonetheless, it is important that DI Scheme is overseen by a coordinator to ensure coherence.

Digital ID Rules and requirements for data localisation

The AIIA notes that s 77 provides for the Rules to make provisions in relations to prohibiting the holding, storing, handling or transferring of such information outside Australia; and the 1,500 penalty units thereafter i.e. $469,000 according to current penalty unit values.

Recommendation: The AIIA notes that the securing information is paramount, and that information can still be under threat within or outside of Australia. It is, therefore, important for the Rules to focus on secure-by-design principles.

Conclusion

The AIIA appreciates the opportunity to make a submission. Should you have any questions about the content of this submission please contact Ms Siew Lee Seow, General Manager, Policy and Media at siewlee@aiia.com.au.

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.

The AIIA represents the depth and breadth of Australia's innovation technology companies. Given the numbers of tech professionals employed by these companies, the AIIA represents a significant portion of the 900,000+ workforce of the Australian technology sector.