12 October 2023

digitalid@finance.gov.au

Department of Finance
Digital ID Taskforce Division
1 Canberra Avenue
Forrest ACT 2603

Dear Associate,

RE: Consultation on the Digital ID Bill and Digital ID Rules

Who we are

Governance Institute of Australia (GIA) is a national membership association, advocating for our network of 43,000 governance and risk management professionals from the listed, unlisted, public, and not-for-profit sectors. As the only Australian provider of chartered governance accreditation, we offer a range of short courses, certificates, and postgraduate study. Our mission is to drive better governance in all organisations, which will in turn create a stronger, better society.

Our members have primary responsibility for developing and implementing governance frameworks in public listed, unlisted, and private companies, as well as the public sector and not-for-profit organisations. They have a thorough working knowledge of the operations of the markets and the needs of investors.

We regularly contribute to the formation of public policy through our interactions with Treasury, ASIC, APRA, ACCC, ASX, ACNC and the ATO. We are a founding member of the ASX Corporate Governance Council. We are also a member of the ASIC Business Advisory Committee, the ASX Business Committee and the ACNC Sector Users Group.

Introduction

GIA's members broadly support the intent of the Digital ID Bill and associated ID Rules. They consider it is critical that the proposed legislation makes it easier for Australians to verify their identity more securely and confidently to safely interact with government and business entities. In an age of cyber threats from increasingly sophisticated networks, it is necessary that individuals' most sensitive personal documents, such as passports, birth certificates and drivers' licence details are exchanged and shared via secure, accessible, and affordable accredited service providers.

We commend the government's efforts to expand on the success of the Australian Government Digital ID System (AGDIS) that operates myGovID providing access to over 130 services by federal, state and territory agencies. There is scope for continual improvement on the ease of accessibility and the ability of individuals to update information. Given the government's current efforts across several reform priorities such as privacy standards and Australia's Cyber Security Strategy our members consider the participation of the private sector is timely.

The transformation to a digital economy is evolving quickly, requiring most if not all individuals to prove their identity to access essential services and undertake dealings with business entities. Current processes are time-consuming, repetitive and place individuals at a high risk of identity theft and fraud,

particularly when vulnerable individuals may be prompted to do so by malicious actors. Individuals' ability to produce adequate ID following a disaster can also be problematic in accessing and applying for disaster relief and services. The move to an effective and secure Digital ID system will streamline many business transactions and improve cybersecurity, limiting the need for copies of personal identification documents and credentials. Our submission provides comments on some key issues our members have identified in relation to the proposals.

Key recommendations

1. **Inclusion, awareness, and affordability**

The objects of the Act outlined in section 3 of the Bill aim to,

> '*Provide individuals with a simple, inclusive and convenient method for verifying their identity in online transactions with government and businesses…*'

While our members support 'digital by default' it is important to ensure equitable access by preserving the ability for those who do not have access to digital means of identity to use traditional means of identifying themselves. A greater number of individuals and businesses may be required to use Digital ID service providers to prove their identity. In this regard, low cost and affordable options should be made available.

There may be members of the community that lack digital literacy, such as elderly Australians. Marginal and vulnerable members of society may be increasingly prompted to maintain digital records of their personal ID to access a greater number of essential services. Investment in education and awareness that targets and supports vulnerable communities may be necessary to instil greater confidence in and use of the Digital ID system, particularly as a greater number of private sector entities come to rely on it. This may also be useful in supporting small businesses and the charitable and not-for-profit sectors to drive uptake.

2. **Co-design approach**

A community driven co-design approach to incorporate the needs of edge cases will act to ensure vulnerable and marginal members of society are included and not excluded from accessing services. There is also scope for trusted third parties to act on the individual's behalf. There may also be merit in cultural consultation to understand the full concept of identity across minority groups. This may be particularly useful for the Aboriginal and Torres Strait Islander communities that possess diverse knowledge, management, and governance systems and pathways for proof of heritage. Sensitivities such as these should be considered as part of a co-design approach to allow full participation of these communities in the digital economy.

3. **Control, access, transparency, and consent**

Incorporating the ability for individuals to act as custodians of their identity promotes transparency and provides individuals greater control of their data, The individual should be provided with the ability to:

- Revoke access to their information and data;
- Grant permission to their data and information;
- Change fluid identity attributes;
- Share elements from their identity with others and;
- Consent for customers to issue, revoke, amend information

Providing individuals with transparency over what data can and can't be used for, and who can and can't handle and use the data is useful in encouraging confidence and uptake. Information which is of a highly

sensitive nature such as biometric information may require additional consent provisions. This may be complemented by a limited retention provision.

4. Verification

As noted in our recent submissions, our members consider verification of the identity of a person executing a document as extremely important in streamlining and securing ordinary business and civil dealings. They also support digital execution using the Australian Government Identity Systems provided there are appropriate safeguards in place to clearly verify identity.[1] Many of our members currently use electronic applications such as Docusign however the integration of a minimum standard for executing and verifying that a document has been validly handled would be a helpful extension of the proposed reforms. These standards could be principles-based, supported by guidance that incorporates the extension of the Digital ID system to private entities. Verification between service providers is also a necessary consideration. Ensuring encryption and security protocols and standards for network traffic between accredited provides and reliant entities is required.

5. International recognition

It is not clear from the proposed Bill whether the digital ID system is intended to be internationally recognised or whether international ID may be held and used in the same way as domestic documents. Interoperability with international standards and internationally issued ID attributes and credentials should be considered. In an internationally exposed, knowledge economy, that is heavily reliant on international skilled migration, the verification of necessary ID and associated qualifications would significantly improve and streamline the processes associated with recruitment and utility of international talent. The benefit of international interoperability is also an important consideration from a regulatory impost perspective as it may go a long way towards reducing duplication of verification processes of international documentation.

6. Monitoring and compliance

The role of the Digital ID regulator is essential to provide confidence in, and support the uptake and use of the system. The currency of information held by the Digital ID system requires it be regularly recertified, particularly in the case of any financial information held. The ability to audit and escalate breaches and potentially suspend participants from the ecosystem is essential to provide confidence in the system. There may be merit in providing and maintaining a public register of accredited ID service providers, so that consumers can verify the accreditation status and currency. Accreditation should also be timestamped, 'as of', 'till end date'. The functions of the Digital ID regulator will therefore require adequate funding and resources to ensure compliance is not a one-off exercise and there is an incorporated complaints function and the ability to escalate and resolve issues brought to its attention quickly. This function could be considered as a regular reporting and review process. Enforcement provisions may provide greater certainty.

7. Penalties

The penalties outlined in the proposed bill may not act as a sufficient deterrent for breaches. Our members consider that any penalties should be graduated in line with the volume and sensitivity of information held and the size of the organisation holding the information.

---

[1] See Submissions Governance Institute of Australia, *Modernising Document Execution: Consultation on proposed reform to the execution of Commonwealth Statutory Declarations*, 26 July 2023 *and* Inquiry into the Commonwealth Statutory Declarations Bill 2023 [Provisions], 21 September 2023.

We provide further comments on the drafting of the Bill in the Attachment. If you have any questions in connection with this Submission, please contact me or Senior Adviser, Policy and Advocacy Daniel.popovski@governanceinstitute.com.au

Yours sincerely,

Megan Motto

CEO

Appendix A – Drafting issues of the Digital ID Bill

Term	Definition	Recommendation
Digital ID	***Digital ID*** of an individual means a distinct electronic representation of the individual that enables the individual to be sufficiently **distinguished** when interacting online with services.	Consider replacing the term 'distinguished' by 'identifiable'.
Identity service provider	**Identity service provider** means an entity that provides, or proposes to provide, a service that: (a) generates, manages, maintains, or verifies information relating to the identity of an individual; and (b) generates, binds, manages, or distributes authenticators to an individual; and (c) binds, manages or distributes authenticators generated by an individual.	Consider interaction with definitions used in other legislation such as *'document verification service'*.
Meaning of attribute of an individual	(1) An **attribute** of an individual means information that is associated with the individual, and includes information that is derived from another attribute. (2) Without limiting subsection (1), an attribute of an individual includes the following: (a) the individual's current or former name; (b) the individual's current or former address; (c) the individual's date of birth; (d) information about whether the individual is alive or dead; (e) the individual's phone number; (f) the individual's email address; (g) if the individual has a digital ID—the time and date the 18 digital ID was created; (h) biometric information of the individual; (i) a restricted attribute of the individual; **(j) information or an opinion about the individual's:** (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or	It may be useful for j) to be redrafted as examples listed under i-vi may not sufficiently identify all 'other' characteristics. Alternatively, it may be useful to insert a definition of an individual's identify as Aboriginal or Torres Strait Islanders as an attribute but not a restricted attribute.

	(vi) sexual orientation or practices.	
Meaning of restricted attribute of an individual	11 Meaning of **restricted attribute** of an individual (1) A restricted attribute of an individual means: (a) health information (within the meaning of the Privacy Act 6 1988) about the individual; or (b) an identifier of the individual that has been issued or assigned by or on behalf of: (i) the Commonwealth, a State or a Territory; or (ii) an authority or agency of the Commonwealth, a State or a Territory; or (iii) a government of a foreign country; or (c) information or an opinion about the individual's criminal record; or (d) information or an opinion about the individual's membership of a professional or trade association; (e) information or an opinion about the individual's membership of a trade union; (f) other information or opinion that is associated with an individual and is prescribed by the Accreditation Rules. (2) Without limiting paragraph (1)(b), an identifier of an individual 22 includes the following: (a) the individual's tax file number (within the meaning of section 202A of the Income Tax Assessment Act 1936); (b) the individual's medicare number (within the meaning of 26 Part VII of the National Health Act 1953); (c) the individual's healthcare identifier (within the meaning of the Healthcare Identifiers Act 2010); (d) if the person holds a driver's licence issued under the law of a State or Territory—the number of that driver's licence.	A restricted attribute may be one or more of those identified in our comments above. As a point for clarification, it is not clear why TFN, Medicare numbers and driver's licence numbers issued by a state or territory are defined as 'restricted attributes' of an individual as these are the documents most sought after in the identification process. It is suggested that part j of the **Meaning of attribute of an individual** be included in the list of restricted attributes of an individual. This will act to align it with **s 41 Collection etc. of certain attributes of individuals is prohibited.**
Application for accreditation	**14 Application for accreditation** (1) An entity covered by subsection (2) may apply to the Digital ID Regulator for accreditation as one of the following kinds of accredited entities: **(a) an accredited attribute service provider;** (b) an accredited identity exchange provider; (c) an accredited identity service provider; (d) an entity that provides a service of a kind prescribed by the 10 Accreditation Rules	It is not clear what the merits or benefits of including a) an accredited **attribute** service provider, would have, given the definition of 'attribute' is broad and may encompass characteristics of individuals that may include prohibited identity markers,

	(2) An **entity** is covered by this section if the entity is one of the following: (a) a body corporate incorporated by or under a law of the Commonwealth or a State or Territory; (b) a registered foreign company within the meaning of the 17 Corporations Act 2001; (c) a Commonwealth entity, or a Commonwealth company, within the meaning of the Public Governance, Performance and Accountability Act 2013; (d) a person or body that is an agency within the meaning of the Freedom of Information Act 1982; (e) a body specified, or the person holding an office specified, in Part I of Schedule 2 to the Freedom of Information Act 1982; (f) a department or authority of a State; (g) a department or authority of a Territory.	such as political beliefs, philosophical opinion, or sexual orientation. It is not clear why the definition of entity is limited to those identified in sub paragraphs a-g, particularly as the aim of the Bill is to expand the scope across private sector entities. We suggest that 'entity' is expanded to include other types of entity.
Digital ID Regulator must decide whether to accredit an entity	Digital ID Regulator must decide whether to accredit an entity (1) This section applies if an entity has made an application under section 14 for accreditation as an accredited entity. (2) The Digital ID Regulator must decide: (a) to accredit the entity; or (b) to refuse to accredit the entity. (3) The Digital ID Regulator must not accredit an entity: **(a) as an accredited attribute service provider unless the entity is an attribute service provider;** or (b) as an accredited identity exchange provider unless the entity is an identity exchange provider; or (c) as an accredited identity service provider unless the entity is an identity service provider; or (d) if Accreditation Rules made for the purposes of paragraph 15 14(1)(d) prescribe services—as an entity that provides services of the kind prescribed unless the entity provides services of that kind. (4) The Digital ID Regulator must not accredit an entity if: (a) a direction under subsection 16(1) (about security) is in force in relation to the entity; or	In line with reasons stated above, we suggest removal of sub-section 3(a). It may be useful to incorporate objective criteria for accreditation into 4(b) rather than the subjective standards of opinion that are used in the current wording.

	(b) if the Digital ID Regulator makes a requirement under paragraph 126(1)(a) in relation to the entity—the Digital ID Regulator is **not satisfied** that the entity has been assessed as being able to comply with this Act; or (c) Accreditation Rules made for the purposes of section 27 require specified criteria to be met and the entity does not meet the criteria; or (d) Accreditation Rules made for the purposes of section 27 require the Digital ID Regulator be satisfied of specified matters and the Digital ID Regulator is not satisfied of those matters.	