Governance Institute of Australia

T +61 2 23 5744 F +61 2 9232 7174
E info@governanceinstitute.com.au
Level 11, 10 Carrington Street,
Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

19 January 2024

economics.sen@aph.gov.au

Senate Standing Committees on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Committee,

RE: Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023

Who we are

Governance Institute of Australia (GIA) is a national membership association that advocates for a community of governance and risk management professionals, equipping over 8,000 members with the tools to drive better governance within their organisation. 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.

Summary of feedback

Consistent with our submission to the Department of Finance in October 2023, Governance Institute is broadly supportive of the intent of a national digital ID scheme. Our members consider it is critical that Government commit to making it easier for Australians to verify their identity securely and confidently so that they can continue to safely interact with Government and business entities. At a time of increasingly sophisticated cyber threats, it is necessary that Australians most sensitive personal documents, passports, birth certificates and drivers' licence details are exchanged, shared, and managed via secure, accessible, and affordable accredited digital service providers. As Digital ID providers become lucrative targets for malicious actors, Government must consider a dedicated regulator that actively monitors and responds to business and individual complaints and concerns. A national campaign is encouraged to raise awareness and confidence in the proposed scheme.

The heightened cyber threat environment requires improved management and protection of ID documents.

We commend the Government's efforts to expand 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 in the ease of accessibility, the ability of individuals to update information and protection of this data from malicious actors. Most if not all Australians are repeatedly

required to prove their identity to access essential services and carry out day-to-day business dealings. Current processes such as providing a photocopy or scan of ID via email are no longer fit-for-purpose in a heightened cyber threat environment. Current processes to validate, manage and store data between individuals, and between businesses and individuals are time-consuming, clunky and place Australians at a higher risk of identity theft and fraud, particularly when vulnerable individuals are actively encouraged to do so by malicious actors.

Building trust, confidence and awareness in the scheme will require a dedicated regulator with sufficient funding and resources to expedite complaints and breaches

The voluntary Accreditation Scheme that enables more Digital ID providers to demonstrate that they meet strong privacy protections, security safeguards and accessibility requirements is a step in the right direction. Our members support the transition from the Trusted Digital Identity Framework (TDIF) to a legislated Accreditation Scheme for public and private sector Digital ID providers. They also consider there should be more stringent penalties as part of the powers of the Regulator outlined in the Bill to suspend, revoke, or cancel accreditations to ensure the Accreditation Rules, privacy protections and safeguards 'have teeth'. The proposed Trust mark for accredited providers should be properly managed to build consumer trust, confidence, and awareness of Digital ID services. There should also be a public campaign accompanying these arrangements so that Australian individuals, business entities and public service providers are clear about the transitional arrangements to a new phased in voluntary digital ID scheme.

Our members support the proposed governance arrangements to establish the Australian Competition and Consumer Commission (ACCC) as an independent Digital ID Regulator to oversee the Accreditation Scheme and the associated enforcement powers that aim to safeguard individuals via civil penalty provisions, enforceable undertakings, and injunctions. They would welcome greater clarity about whether the ACCC will manage and operate these functions separately to the Office of the Australian Information Commissioner which will continue to advise on and enforce privacy protections and complaint handling functions for privacy breaches. The consider a preferable approach would be to establish an amalgamated independent regulator with combined functions and adequate funding and resources, to enable a clear pathway for complaint raising and handling processes and procedures for individuals and businesses. The Office of the Australian Information Commissioner would continue to play an important role on advising and enforcing broader privacy protections, and complaint handling functions for privacy breaches. However, given the seriousness and criticality of any significant Digital ID breach there should be a dedicated complaints handling regulator alongside the Digital ID scheme. Any dedicated Digital ID regulator should be funded and resourced to enable it to act expeditiously on complaints and enquiries raised by individuals and businesses.

The currency of the information held by the Digital ID system will be important and will need to be regularly recertified, particularly in the case of any financial information. The ability to audit and escalate breaches and potentially suspend participants from the ecosystem is essential to provide confidence in the system. This will require the proposed regulator to take a very active role, such as providing and maintaining a public register of accredited ID service providers, so that consumers can verify 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. There should also be a 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.

The scheme should be inclusive and affordable for all Australians

We have previously emphasised the need for an inclusive and affordable approach that places Australians in control of their identity, safeguards access, as well as providing transparency and informed consent. Individuals should have the ability to revoke access to their information and data, grant permission to their information and data, change fluid identity attributes, share elements of their identity with others and allow individuals to issue, revoke and amend aspects of their personal information. Identity providers that help

set up and manage Digital ID should be affordable and easy to access for all Australians including those from disadvantaged communities, or those with low digital literacy skills.

Digital ID service providers should be listed as critical asset holders under the SOCI Act

We support Government efforts to reduce the burden on businesses to collect, store, and manage sensitive personal data for the purchase of goods and services that require a form of identity verification helping to reduce the incidence and threat of cyber-attacks. However, this will result in a commensurate increase in risk placed on Digital ID service providers as they become increasingly targeted by malicious actors. Digital ID service providers should be mandated to report under the Security of Critical Infrastructure Act 2018 (SOCI) that requires positive security obligations and enhanced cyber security obligations.

International interoperability to reduce duplication of verification processes of international documentation is encouraged

It is not clear whether the Digital ID scheme 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 and students, the verification of necessary ID and associated qualifications would significantly improve and streamline recruitment of international talent. The benefit of international interoperability is also an important consideration from a regulatory impost perspective as it may assist in reducing the duplication of verification processes of international documentation.

Finally, we encourage the Government to publicise a cost-benefit analysis that supports the introduction of the scheme. If you have any questions in connection with this Submission, please contact me or Senior Adviser, Policy and Advocacy [redacted]

Yours faithfully,

[redacted]

Catherine Maxwell
General Manager, Policy and Advocacy