[redacted]

**Submission: draft *Digital ID Bill 2023* (draft Bill), *Digital ID Rules 2024***

The Digital Industry Group Inc. (DIGI) thanks you for the opportunity to provide our views on the proposed Digital ID Bill 2023 (draft Bill), Digital ID Rules 2024 (draft Rules) and draft Digital ID Accreditation Rules 2024 (draft Accreditation Rules) (and jointly 'draft legislation and rules').

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, Discord, eBay, Google, Linktree, Meta, Spotify, Snap, TikTok, Twitch, X (f.k.a Twitter) and Yahoo. DIGI's vision is a thriving Australian digitally enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI shares the Government's strong commitment to providing Australian end-users with a secure, convenient, voluntary and privacy protected way to verify their ID online. We therefore support the development of a voluntary accreditation scheme of Digital ID service providers, and an Australian Government Digital ID System that will be expanded over time to include private sector organisations that choose to participate.

**Voluntary Nature of Mechanisms**

At the outset, we want to emphasise the crucial importance of the voluntary nature of the proposed mechanisms in relation to identity establishment, verification and management set out of the draft legislation and rules. We believe that it is important for the Australian Government to adopt and maintain policy settings that support an open and competitive market for digital identification services, which in our view is the best way to incentivise investment, encourage innovation and ensure that a range of convenient, secure, and cost effective solutions are available to digitally-enabled services operating across the digital economy. From a security perspective, we also believe that such an approach that enables the development of a decentralised digital identity architecture, rather than a centralised system is preferable, given the greater vulnerability of centralised architectures to cyber-attacks and privacy breaches.

**Key Recommendations**

We have engaged in close dialogue with our fellow industry association, Communications Alliance, who has been deeply engaged in the development of the draft legislation and rules. We wish to convey our

general support for the Communications Alliance submission, including the following key recommendations:

1. The prohibition concerning the use of personal information 'about an individual that is in the entity's possession or control' for 'prohibited marketing purposes' in section 52 should be amended, so that it only applies only to *personal information that the accredited entity has come into possession or control of solely for the purpose of providing the accredited service*. This is necessary to ensure that an accredited entity is able to use personal information that it has legitimately obtained for marketing purposes independently of its activities as an accredited entity. For example, when a user independently opts-in to marketing emails.
2. Further consideration should be given to the drafting of section 52 to ensure that it does not prevent the ongoing practical uses of certain types of information that benefit users, for example, the use of technical identifiers to save the users preferences on the primary service.
3. We encourage the Government to carefully consider the scope and impact of the limitations in the Bill concerning the collections, use and disclosure of biometric information of an individual in sections 45 and the circumstances in which the use of such biometric information may be permissible for preventing or investigating a digital ID fraud incident in section 46. In particular, the definition of 'digital fraud incident' is restricted to circumstances in which a digital ID is suspected of being compromised or rendered unreliable. We note that the requirement that the ID be suspected of being unreliable or rendered unreliable would operate to prevent routine use of such information for detecting/preventing scam operations, and consideration should be given to removing this requirement to improve the overall security of the digital ecosystem for end-users.
4. The Digital ID Regulator has an overly broad discretion in section 69 to suspend a participant in the system if the regulator reasonably believes that there has been a cyber security incident involving the entity or reasonably believes that such an incident is 'imminent'. We consider there should be greater clarity concerning the circumstances in which the regulator is able to exercise these powers given the serious consequences of suspending an entity's participation in the system, especially where that would result in the entity from being unable to provide any service for an extended period. Additionally, there is a need to consider the implications on industry where there is a monopoly or dominant provider of ID services exiting the market - and how this can be addressed. Further, the definition of cyber-security incidents is also overly broad and covers incidents that do not directly impact on the digital ID system. We consider this definition should be limited to 'systems, services and networks that, if compromised, have the capacity to pose a risk to the integrity of the digital ID system.'

[redacted]

[redacted]