REINSW
for members since 1910

Draft Digital ID Rules 2024 (Cth), Draft Digital ID (Accreditation) Rules 2024 (Cth) and Draft Digital ID (Accreditation) Data Standards 2024

The Real Estate Institute of New South Wales Limited

Submission on the *Draft Digital ID Rules 2024 (Cth), Draft Digital ID (Accreditation) Rules 2024 (Cth) and Draft Digital ID (Accreditation) Data Standards 2024*

3 July 2024

TO: **Digital ID Legislation Engagement team**
Digital ID Taskforce
By email: digitalidlegislationengagement@finance.gov.au

1. Introduction

This Submission has been prepared by The Real Estate Institute of New South Wales Limited (**REINSW**) and is in response to the draft *Digital ID Rules 2024*, the draft *Digital ID (Accreditation) Rules 2024* and the draft *Digital ID (Accreditation) Data Standards 2024* (**Digital ID Rules and Standards**).

REINSW is the largest professional association of real estate agents and other property professionals in New South Wales. REINSW seeks to promote the interests of its members and the property sector on property-related issues. In doing so, REINSW plays a substantial role in the formation of regulatory policy in New South Wales.

This Submission outlines issues and recommendations for Government to consider in relation to the Digital ID Rules and Standards.

2. Voluntary Participation for Digital ID

Section 74(1) of the *Digital ID Act 2024* (Cth) provides that an individual cannot be required to "create" or "use" digital ID when accessing a service.

Section 74(1A) of the *Digital ID Act* also prohibits offering of services that would not be "reasonably accessible" without use of digital ID or would be provided on "substantially less favourable terms" compared to if that individual used digital ID. However, section 74(2) of the *Digital ID Act* provides an exception where another reasonably accessible alternative service that "does not result in the other service being provided on substantially less favourable terms" is offered.

While REINSW supports voluntary use of digital ID, it questions how such a provision will work in practice. Its view is that, in some scenarios, the nature of the transaction or an individual's circumstances will mean that use of digital ID is the only viable option – even if it is technically voluntary.

For instance, the exception in section 74(2) of the *Digital ID Act* provides an example where a bank, which requires new customers to verify their identity when opening a bank account, does not contravene section 74(1A) because an individual can choose to have their identity verified at their local branch instead. However, in practice, attending a local bank branch might not be a viable option where:

- the service is time sensitive and the bank branch is not open because it is outside of trading hours or a public holiday;
- where a person lives in a rural area and their nearest bank branch is far away from where they live; or
- where their bank's model is online based. For example, ING is a branchless bank who only has one physical branch in the Sydney CBD.

In each of the above scenarios, an alternative verification method exists which appears, on the face of it, to be reasonably accessible. However, in practice, it might not be accessible to

all persons all the time and so individuals may need to resort to the use of digital ID even if this is not their preference.

Furthermore, in some circumstances, setting up and connecting digital ID with the relevant service provider might not be straightforward or instantaneous. REINSW is aware that some individuals have experienced technical difficulties setting up MyGOV ID. REINSW is concerned that without a viable verification method, technical difficulties associated with setting up digital ID, has the potential to delay important and time sensitive transactions (such as real estate transactions) to the potential detriment and expense of parties involved. ***REINSW recommends*** that that the Digital ID Rules and Standards address in more detail how this exemption will work in practice to ensure that persons can effectively and promptly access other verification methods where an individual does not want to, or is unable to use, digital ID.

REINSW also notes that section 74(4) of the *Digital ID Act* grants the Digital ID Regulator the discretion to grant an exemption to a participating relying party. REINSW is concerned that this means that there may be transactions which require individuals to use digital ID as the only option to access a service. In circumstances where individuals are unable to opt out of digital ID (either because the service provider has an exemption or surrounding circumstances do not make alternative verification methods viable in practice), ***REINSW recommends*** that the Digital ID Rules and Standards implement additional safeguards or data collection minimisation practices to protect individuals' data. For example, ***REINSW recommends*** that rule 5.4 of the draft *Digital ID (Accreditation) Rules 2024* which allows for one-off digital IDs to be generated where an individual's attributes are not retained once disclosed to a relying party (unless required by law) could apply to such transactions.

3. Documentation Verification Service Methods

As part of the consultation process, REINSW recently attended Government's roundtable to discuss the Digital ID Rules and Standards. During that roundtable, several attendees who were well versed in biometric technology (including one attendee who was co-writing a white paper with the International Criminal Police Organisation) were of the view that the document verification service within the digital ID framework was not as effective as other technologies available. For example, it was mentioned in that roundtable that the document verification service used within the digital ID framework only had a 79% success rate of detecting deep fakes, whereas other available technologies had a success rate of 99%.

While REINSW is not familiar with the technical intricacies of biometric and document verification service technology, its view is that it is essential that the technologies used as part of the Australian Government Digital ID System (**Digital ID System**) should be as robust as possible to protect the personal information of individuals from fraud, cyber security incidents and unauthorised disclosure. This is especially so, given that promoting "privacy and the security of personal information used to verify the identity or attributes of individuals" is one of the *Digital ID Act's* objectives. ***REINSW recommends*** that Government consult further with experts to ensure the biometric and document verification service technology used adequately protects individuals' data that is provided as part of the Digital ID System.

4. Impact on Vulnerable Persons

REINSW recommends that Government further consider how the Digital ID System might impact vulnerable members of society (for example, victims of domestic violence or elder abuse). Because digital ID will be able to be used to verify a person's identity across a range of public and private sector entities, REINSW is concerned that this could be exploited by a perpetrator when exercising coercive control over the victim with potentially serious consequences. Furthermore, it may be easier for a perpetrator to track down a victim where an individual's personal information and data will be stored in a centralised system. ***REINSW recommends*** that the Digital ID Rules and Standards consider and implement safeguards which would protect vulnerable members of society from misuse of personal information in such circumstances.

5. Summary

In summary, ***REINSW recommends*** that:

- the Digital ID Rules and Standards address in more detail how the exemption in section 74(2) of the *Digital ID Act* will work in practice to ensure that persons can effectively and promptly access other verification methods where an individual does not want to, or is unable to use, digital ID;

- the Digital ID Rules and Standards implement additional safeguards or data collection minimisation practices to protect individuals' data (for example, ***REINSW recommends*** that rule 5.4 of the draft *Digital ID (Accreditation) Rules 2024* which allows for one-off digital IDs to be generated where an individual's attributes are not retained once disclosed to a relying party (unless required by law) could apply to such transactions);

- Government consults further with experts to ensure the biometric and document verification service technology used adequately protects individuals' data that is provided as part of the Digital ID System; and

- Government further considers how the Digital ID System might impact vulnerable members of society and that the Digital ID Rules and Standards consider and implement safeguards which would protect vulnerable members of society from misuse of personal information in such circumstances.

6. Conclusion

REINSW has considered the draft Digital ID Rules and Standards and has provided its comments above, aiming to provide input on as many pertinent aspects of the draft Digital ID Rules and Standards as possible. However, REINSW's resources are very limited and, accordingly, it does not have the capacity to undertake a thorough review and is unable to exhaustively investigate all potential issues in this Submission. Nonetheless, REINSW has identified a number of matters that it believes will cause significant consumer detriment, some of which appear above.

REINSW appreciates the opportunity to provide this Submission and would be pleased to discuss it further, if required.

Yours faithfully

Tim McKibbin
Chief Executive Officer