The Real Estate Institute of Australia
16 Thesiger Court I PO Box 234, Deakin ACT 2600
Phone 02 6282 4277 I Fax 02 6285 2444
www.reia.com.au I reia@reia.com.au

REIA
REAL ESTATE INSTITUTE OF AUSTRALIA

25 June 2024

Department of Finance
One Canberra Avenue
Forrest, ACT 2603

Via online lodgement

REIA Submission: 2024 Digital ID Rules, Accreditation Rules and Data Standards

To whom it may concern,

The Real Estate Institute of Australia (REIA) serves as the national representative body for the real estate profession in Australia.

Since our establishment in 1924, REIA has focused primarily on advocating for policies that underpin a thriving real estate industry. Our membership comprises the State and Territory Real Estate Institutes (REIs), which collectively represent approximately 85% of Australian real estate agencies, encompassing 46,793 businesses.

Presently, REIA is engaged in activities related to policy and political endeavors, media advocacy, market research, industry excellence, and national leadership, all aimed at supporting real estate practitioners and agencies.

Notably, the real estate sector stands out as a significant component of the Australian economy, catering to almost all Australians primarily through small businesses. To contextualize this, there exist 44,000 real estate agencies across Australia, with 99% classified as small businesses.

At the same time our consumer base is considerable, with our outreach estimated to be:

- 6.9 million Australians helped into home ownership or rentals each year.
- $350 billion in home sales settled the last recorded financial period.
- $78 billion in rent receipts collected annually.
- $3 trillion in rental assets under management.
- Combined residential real estate asset value of $9.3 trillion.
- Combined commercial real estate asset value of around $1 trillion.

REIA Policy Position

REIA advocates for a best practice approach in safeguarding our digital domain, our policy position includes ensuring the safety of members and consumers amidst rapid technological advancements. We emphasize the necessity of responsible regulation to protect businesses, practitioners, and consumers. Additionally, we advocate for institutions to provide essential resources such as education, toolkits, and response plans for navigating the digital landscape, and to ensure that third-party providers uphold rigorous cybersecurity and data use standards.

This represents a clear and direct policy stance that aligns with the strategic objectives outlined in our Getting Real 2.0 strategic policy document. Therefore, REIA welcomes the opportunity to provide a submission on the 2024 Digital ID rules, Digital ID Accreditation Rules and Accreditation Data Standards.

Submission to consultation questions

REIA has elected to respond to the specific consultation questions as noted in the feedback template below:

Digital ID Rules

Consultation question for Rule 3.3 – The requirements included in this rule 3.3 are based on existing requirements applicable to Government entities seeking to onboard to the Australian Government Digital ID System. They are designed to ensure that the System Administrator and the government relying parties reach an agreement prior to onboarding on how different types of incidents relating to the AGDIS are managed, so that if an incident occurs these can be resolved effectively. We are seeking feedback on how to achieve this coordinated response in future phases of the AGDIS rollout, where non-Government organisations who may not have large fraud and security teams may find these requirements difficult to meet.

How would you consider clarifying these rules for non-government organisations while still maintaining strong minimum security and fraud protections for individuals who may use their digital ID to access that relying party service?

REIA acknowledges the importance of establishing robust incident management protocols to ensure the security and integrity of the Australian Government Digital ID System (AGDIS).

Key considerations to clarifying these rules to non-government organisations while still maintaining strong minimum security and fraud protections for individuals who may use their digital ID to access that relying party service must include the following:

- Government to provide business offsets or subsidies that align with the agency's risk profile and resource availability.
- Provision of centralized workflow and enquiry management system.
- Provision of training programs and resources that are readily accessible and user-friendly to ensure basic compliance requirements are understood and met.
- Flexibility to be provided for organisations to meet the security requirements in a manner that aligns with their operational capabilities.

Consultation question for rule 4.2 – This rule is based on reporting requirements that are currently used in the Australian Government Digital ID System. Do you have any suggested changes to this rule supporting the relevant regulator in accessing the necessary information to undertake investigations into cyber security or fraud incidents that could occur within the Australian Government Digital ID System?

REIA advocates for a clear and transparent reporting mechanism along with clear guidelines on reporting obligations to be established for organisations. While ensuring that regulators have access to necessary information, it is crucial to maintain confidentiality and protect sensitive data. Robust data protection measures should be implemented to safeguard the privacy of individuals and entities involved in the incidents.

This is particularly true given that sensitive personal information is stored throughout the entire real estate transaction chain and real estate agencies are required to act in the best interests of their clients.

Consultation question for rule 6.2 – The record keeping provisions required for the logging of information in relation to Australian Government Digital ID System transactions and other system information required by rule 6.2 in the proposed Digital ID Rules has been amended to 6 years. This is different from the proposed Accreditation Rules requirement for logging the same information under rule 4.20. Rule 4.20 in the proposed Accreditation Rules maintains that logs required for that rule are required to be kept for 3 years.

- *Is 6 years an appropriate timeframe to retain the logging and transaction information required by rule 6.2 in the proposed Digital ID Rules in relation to transactions and personal information on the Australian Government Digital ID System?*
- *What do you consider an appropriate minimum timeframe for the retention of this type of information?*

REIA notes that this is an appropriate timeframe that is proposed given that the Health Records and Information Privacy At, Corporations Act 2001 and Fair Work Act 2009 all require a record retention length of 7 years. Considering the nature of the information and the potential implications of security and fraud incidents, REIA proposes that the minimum retention period should not be less than five years.

REIA understands that other kinds of personal information such as an individual's name or restricted attributes collected for the purpose of a Digital ID are not required to be kept under the logging requirements in rule 4.20 of the proposed Accreditation Rules.

Consultation question for Chapter 7 – The interim liability arrangements in Chapter 7 are prescribed for the initial phases of the Australian Government Digital ID System, where participants are Australian or state and territory government entities.
The liability arrangements in the proposed Digital ID Rules will be reviewed prior to the expansion of the Australian Government Digital ID System to the private sector.

- *What kinds of liability arrangements would your organisation expect to see operational on Australian Government Digital ID System?*
- *Are there any existing liability frameworks that the Digital ID Rules could draw from?*

The liability arrangements should be clearly defined to include the responsibilities and liabilities of all parties involved, including identity providers, relying parties, and the system administrator. This clarity will help prevent disputes and ensure accountability.

There should be reasonable caps on liability to protect smaller entities and ensure that the liability framework does not become a barrier to participation in the Digital ID System, along with relevant indemnity provisions in place.

Digital ID Accreditation Rules

General questions – Accreditation Rules and data retention periods for personal information:
Retention of personal information collected from an individual is managed through an accredited entity's own policies and requirements of its services as well as its tolerance for security and fraud risks associated with the retention of that information (e.g. the longer it is retained, the more at risk that information may be of being breached).

- *Should the Accreditation Rules set out a maximum data retention period for an individual's personal information? For example, that an accredited entity must delete personal information after a period of time if an account becomes dormant. What should that period of time be?*

REIA notes the importance of balancing data retention with the risks associated with prolonged storage of personal information. Organizations should establish retention policies based on the principle of not keeping personal information longer than necessary for the purpose for which it was collected.

This should be a maximum of 5 years which is long enough to accommodate potential reactivation of accounts while minimizing risks associated with extended data storage.

General questions – Accreditation Rules and barriers to entry for the accreditation scheme:
The Accreditation Rules are a set of minimum controls that are designed to address Digital ID specific risks to individuals and relying parties. Some previous feedback has indicated that because of the technical nature and complexity of the Accreditation Rules and Accreditation Data Standards, that there is a high cost of entry to the accreditation scheme due to the kinds of controls accredited entities are expected to implement.

- *If the Accreditation Rules were to be simplified, which rules would you suggest be removed?*
    - *If you are suggesting removal of a rule, how would you recommend mitigating the risk that rule was designed to address?*
- *Are there any other standards that are not already incorporated into the rules that you suggest should be considered?*

The rules that should be considered for potential removal or simplification are those that exhibit redundant controls, excessively technical requirements, and costly implementation measures. To identify such rules, a comprehensive risk assessment should be conducted, drawing on industry best practices and considering emerging threats in digital identity management.

Incorporating additional standards should be done with a focus on complementarity rather than duplication. Each standard should add value by addressing specific aspects of security, privacy, usability, or interoperability that are critical to the accreditation scheme's objectives. Regular consultation with stakeholders and industry experts can provide valuable insights into which standards are most relevant and beneficial for enhancing the accreditation framework.

Consultation Question for Rule 3.8 – The penetration testing rule has been updated to better clarify the scope and requirements of a penetration test, including what is required to be tested and what kind of testing must be included in a penetration test. Do you have any feedback regarding this requirement?

Penetration testing requirements should be clear, practical, and aligned with industry standards, while also considering the operational impact on accredited entities and opportunities for continuous improvement.

Consultation question for Rule 4.41 – Some feedback has indicated that the rules should not set a timeframe for enduring consent to expire and instead allow accredited entities to set their own policies for the expiry of enduring consent dependent on the service that is being provided. Do you think the rules should set a timeframe for enduring consent to expire? What should that timeframe be?

Accredited entities should have the flexibility to establish their own policies for consent expiry based on the nature of the service provided. REIA would like to highlight that a fixed timeframe for enduring consent may not align with the diverse timelines and needs of our clients, as real estate transactions can vary significantly in complexity and duration.

REIA Conclusion

REIA would like to point out that our submission emphasizes the importance of balancing regulatory compliance with practical considerations specific to the real estate industry.

This approach supports our commitment to ensuring that Australians are provided with the appropriate support to get into more homes while safeguarding their privacy and trust in the evolving digital landscape of real estate.

Should you require further information, I can be contacted on 0448 692 245 or anna.neelagama@reia.com.au.

Yours sincerely,

Anna Neelagama
Chief Executive Officer
The Real Estate Institute of Australia