Australian Information
Industry Association

Australian Information Industry Association

Submission on the

Digital ID Rules and Accreditation Rules Consultation

17 October 2025

About the AIIA

The Australian Information Industry Association (AIIA) is the nation's peak body for those in the digital ecosystem, leading strategic policy and advocacy to shape a thriving digital sector. Through strong engagement with government, industry, and the broader community, the AIIA ensures the voice of its members informs decision-making on technology, innovation, and digital capability.

Membership provides direct access to influential networks, premium events, and opportunities to collaborate on initiatives with the sector's best and brightest to drive industry growth, improve productivity, and secure Australia's place as a global technology leader. AIIA members access real collaboration, real connections, and real outcomes.

Introduction

The AIIA appreciates the opportunity to provide feedback on 2025 Digital ID Rules and Accreditation Rules consultation.

We strongly support the ongoing development of a secure, privacy-protective, and interoperable national Digital ID System. These proposed amendments represent an important step in strengthening user protections, clarifying system governance, and improving alignment between regulatory frameworks.

Redress Framework

The AIIA commends the Department of Finance ("Department") for introducing a formal redress framework for the Australian Government Digital ID System (AGDIS). We support the establishment of this framework and believe this initiative will bolster existing incident remediation requirements by ensuring that individuals who suffer harm or inconvenience through the misuse or compromise of their digital identity have clear pathways for support and resolution. Strengthening redress mechanisms in this way will improve outcomes for users and enhance public confidence that any issues with the Digital ID system can be fairly addressed.

To achieve the desired clarity and consistency in incident notification, the AIIA recommends aligning the Digital ID Rules' notification requirements with the Privacy Act's[1] Notifiable Data Breaches (NDB) scheme. The NDB scheme is an established framework that many entities in the Digital ID ecosystem are already subject to, and it provides a well-understood standard for when data breaches must be reported to individuals and regulators.

[1] Privacy Act 1988 (Cth).

Aligning the Digital ID incident notification trigger with the NDB scheme's "likely risk of serious harm"[2] threshold would provide several benefits. Firstly, entities operating within AGDIS would follow one clear standard for breach notification, rather than juggling separate criteria for the Digital ID system versus the Privacy Act. Most accredited participants are already bound by the Privacy Act; a consistent approach means they do not have conflicting or duplicative obligations. As the AIIA has previously noted, overlapping reporting requirements across different regimes can become "complicated and could potentially result in confusion, undermining the effectiveness of each reporting scheme."[3] By mirroring the NDB scheme, the Digital ID Rules can avoid introducing slightly different or additional thresholds that might confuse participants. Secondly, alignment with the NDB scheme would provide certainty for all stakeholders. Both providers and users would know that a serious incident affecting personal information in the Digital ID system will be handled with the same urgency and transparency as any other data breach in Australia's regulatory environment. This certainty reduces ambiguity and helps entities build incident response processes that meet both Digital ID and Privacy Act requirements simultaneously.

Coordinating the Digital ID incident response framework with the NDB scheme in this way will ensure a seamless and familiar approach. Entities would be able to use their existing breach assessment processes to determine when to notify users of a Digital ID incident, rather than having to apply a new test.

Reportable Incident Investigations and Oversight

The AIIA supports the intent of the proposed amendments to strengthen the System Administrator's oversight of cyber security and digital ID fraud incidents. This is an important step towards ensuring consistency, accountability, and timely resolution across the system.

However, the amendments to Rule 4.2, specifically new subrules (7) to (9), would benefit from further clarification to ensure their effective and proportionate application. As currently drafted, subrule 4.2(7) provides that "the System Administrator *may* direct any entity of a kind mentioned in subrule (1) who has interacted with a digital ID affected by the incident to conduct an investigation into the incident." While this introduces a valuable mechanism to improve coordination and oversight, the open-ended wording risks uncertainty about when such directions are appropriate, the objectives of the investigation, and the expectations placed on accredited entities.

---

[2] Ibid s 26WE(2)(b).
[3] Australian Information Industry Association, Submission to the Department of Finance: Feedback on Digital ID Rules, Digital ID Accreditation Rules and Accreditation Data Standards (28 June 2024) 4.

To support consistent interpretation and implementation, the AIIA recommends that the rule and accompanying guidance:

1. **Clarify the purpose of investigations**: The rule should specify the objectives of a directed investigation, including whether it is intended to determine the root cause of the incident, assess systemic vulnerabilities, confirm the adequacy of remediation measures, or support potential compliance or redress actions. Clear articulation of purpose will assist both the System Administrator and accredited entities in ensuring that investigative resources are appropriately directed and proportionate to the incident's impact.

2. **Define the circumstances under which a direction would be issued**: The rule should outline the threshold or criteria for when the System Administrator "may" direct an entity to conduct an investigation. This could include consideration of the scale or severity of the incident, the sensitivity of affected data, whether multiple entities were involved, or whether there is a risk of systemic compromise.

3. **Provide guidance on the scope and expectations of investigations**: Entities should have a clear understanding of what a directed investigation entails, including procedural requirements, expected deliverables, and reporting timelines. This could encompass guidance on the level of technical depth required, whether external forensic expertise is expected or permitted, and how investigation findings will be used by the System Administrator.

Clarifying these aspects would promote a consistent and transparent approach across accredited entities and ensure that the System Administrator's new powers are exercised in a manner proportionate to the nature and seriousness of incidents. It would also enable entities to align their internal incident response frameworks with the System Administrator's expectations, minimising uncertainty and duplication while strengthening confidence in the Digital ID System's capacity to manage and remediate cyber incidents effectively.

Conclusion

The AIIA welcomes the Department's continued commitment to refining Australia's Digital ID framework through measured and practical regulatory amendments. The proposed reforms represent a positive step towards strengthening public confidence, ensuring accountability, and improving coherence across the broader digital trust ecosystem.

The AIIA appreciates the opportunity to contribute to this consultation and looks forward to continued engagement with the Department as the Digital ID framework evolves to support a secure, trusted, and innovation-enabling environment for all participants. Should

you require further information, please contact Mr David Makaryan, Advisor, Policy and Media, at david@aiia.com.au.

Yours sincerely

Elizabeth Whitelock
Interim CEO, AIIA