

## Key questions on the Digital ID legislation and Digital ID Rules

Page # of guide	Question	Your response
14	What other types of Digital ID service should be included in the legislation, either now or in future?	<p>First nations are the most disenfranchised groups in Australia when it comes to digital and physical ID. The history of Australia for first nations people since colonisation has meant an entire population unable to be identified as First nations people in their own communities in a way that is culturally safe and wholly inclusive.</p> <p>This has resulted in the inability to participate equally and attain independent opportunities without the control of identity and credentials by third parties. The complex nature of this issues in Australia has meant identity assertion and document control has played a major factor in loss of self-determination.</p> <p>Digital identity should incorporate diverse ways of identification. The identity legislation should be flexible enough to be inclusive of the inherent values underpinning culture identity, community identity, and heritage identity.</p> <p>The right to hold an inclusive diverse identification as an Indigenous person, is the key to the door to unlock human right to self-determination.</p>

Page # of guide	Question	Your response
		<p>To achieve this, we recommend four ways to achieve inclusive identity management for the government consider in legislation, aiming to transition first nations to digital identification with culturally inclusive systems of identification.</p> <ol style="list-style-type: none"> <li>1. Legislation recognises non-government providers servicing Aboriginality identification solutions.</li> <li>2. Accrediting unique perspectives for Indigenous digital ID services.</li> <li>3. Legislation should be inclusive of the needs of regional and remote Australians, ensuring choice and accessibility to non-government providers.</li> <li>4. Legislation should be flexible to offer services culturally inclusive of Indigenous people's unique perspectives and relationships of identity.</li> </ol>
14	Does the Minister's rule-making power to include new services over time provide appropriate flexibility to add new types of Digital ID services? If not, why not?	<ul style="list-style-type: none"> <li>• There needs to be consideration for flexibility to evolve technology for the purposes of humanity.</li> <li>• The flexibility for digital ID in regional and remote communities may not entirely be 100percent digital. The flexibility of unique services catering for the inclusion of these communities should also be under the consideration of the Minister's rule making power.</li> <li>• To be inclusive of services that improve Indigenous cultural perspectives for access to digital Aboriginality ID. Ensuring ways of protecting cultural safety and asserting Aboriginality in a meaningful way serviced by Indigenous accredited services.</li> </ul>

Page # of guide	Question	Your response
16	Is the Regulator's power to impose conditions on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the Regulator's power to impose conditions on accreditation be improved?	
16	Is the application for accreditation process appropriate, or should other matters be included, or some excluded?	<ul style="list-style-type: none"> <li>• The system should consider specialised categories such as accrediting diverse ID perspectives for the digitally excluded populations.</li> <li>• It is important for government to include first nation perspectives for diverse ways of identification, as demonstrated in ██████ (digital identity for diversity).</li> <li>• Indigenous ID accredited provider should be considered in first instance as attribute providers and/ or identity providers. Included in matters relating to governments Indigenous procurement policy, Indigenous identification (Aboriginality) certifications, and service diversity conditions such as closing the gap targeted schemes.</li> </ul>
17	Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?	
21	Are the additional privacy safeguards sufficiently robust, clear and practical?	

Page # of guide	Question	Your response
21	Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric information?	
21	Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?	
23	What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?	<p>Recommend an age of 16years of age.</p> <p>Factors of ID usage dependent on age, factors under consideration include:</p> <ul style="list-style-type: none"> <li>• Age of learner driving license</li> <li>• Secondary school apprenticeships</li> <li>• Minimum age of criminal liability in Australia is 14yrs.</li> <li>• Senior level Year 11 in secondary education</li> <li>• Developmental age in search of an identity to</li> <li>• Transitional age for youth workforce commencing partial employment.</li> <li>• Required to open banking account for employment.</li> <li>• Transition out of secondary school averages 16,17,18 years.</li> </ul>

Page # of guide	Question	Your response
25	What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?	<p>Take steps to ensure inclusion of existing first nations services offering digital ID service solutions are uniquely placed in the AGDIS.</p> <p>Take necessary steps to be fully inclusive of Indigenous digital ID services for accreditation Indigenous entities who provide significant value in delivering services for procurement, compliance, cultural inclusive standards.</p>
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	That Indigenous peoples and other marginalised groups using services in regional and remote Australia are under considered for choice and digital ID expansion.
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	<p>It would ensure that Indigenous ID services such as ██████████ is supported by governments for the inclusion of Indigenous peoples.</p> <p>The important role of ██████████ as a digital ID offers an opportunity to impact the market with greater efficiency and accessibility to an eco-system where we as an Indigenous digital ID service participates - ██████████ the marketplace.</p> <p>Helps to drive greater participation and productivity for all Australians.</p>
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?	<p>The voluntary use of digital ID services makes it possible to provide informed choices by the individual.</p> <p>Services provide the opportunity outside of government with the flexibility to target needs of consumers in ways government are unable too. Providing under served populations with choice, particularly Indigenous populations with reduced access to choose. Capable of making informed choices to access ID in a way that better serves their needs from Indigenous accredited services.</p>
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	

Page # of guide	Question	Your response
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	
34	Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?	
34	What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?	