

2023 Digital ID Bill and Rules

SUBMISSIONS BY

PRASHANT SINGH

FOUNDER & NATIONAL CHAIRPERSON

INDIAN AUSTRALIAN TECHNOLOGY FORUM



Digital ID means better , secure and reliable digital experiences for Australians

Recent cyber breaches have highlighted the risk in current systems where multiple copies of PII are held by corporations and groups.

Digital ID will make it easier to access citizen services and will serve as the backbone of our digital economy.

I have long advocated for the introduction of Digital ID and welcome the opportunity to contribute.

I applaud the team and leadership for putting this legislation forth in 2023; it will lay the solid foundation our country requires to ensure our digital future.

Prashant Singh

Founder –Indian Australia Technology Forum Inc
Perth - Australia

Australia's Digital ID System


Key questions on the Digital ID legislation and Digital ID Rules

Your name	Prashant Singh
Your organisation	Founder- Indian Australian Technology Forum Inc

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?	Universal Digital Citizen ID, linked to biometric, should also be considered as part of the future legislation. Various examples of such Digital ID are used by countries across the world to underpin Digital Services.
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?	Minister rule making power should allow to include future new services
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	Yes, it is an appropriate mechanism

Page # of guide	Question	Your response
	accreditation be improved?	
16	Is the application for accreditation process appropriate, or should other matters be included or some excluded?	Yes, it is appropriate
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?	Maximum penalties should be proportional to the company's revenue generated if we want penalties to be an appropriate deterrent for big companies. We have seen overseas examples of companies getting a slap on the wrist fines for privacy breaches and writing it off from future profits and getting away.
21	Are the additional privacy safeguards sufficiently robust, clear and practical?	Yes
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?	Yes. Law enforcement and national security matters should be given that access.
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?	Maximum penalties should be proportional to the company's revenue generated if we want penalties to be an appropriate deterrent for big companies. We have seen overseas examples of companies getting a slap on the wrist fines for privacy breaches and writing it off from future profits and getting away.
23	What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?	13 years should be fine. People with limited access to digital services, Cultural diversity and other regional communities' groups should be consulted and Digital ID age provisions should be made appropriate to ensure these Australian communities are not disadvantaged
25	What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and	Technical standards, Interoperability, User Feedback, Conducting Pilots Cyber Security capabilities, Data Sovereignty, Data Security, Business Continuity Planning, Disaster Recovery, Natural Disaster event, Cyber

Page # of guide	Question	Your response
	accredited entities?	Resilience testing, Service Support, Usage of AI in digital services are few things to consider. This will ensure Digital ID services are matured enough before wider rollout.
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	Technical standards, Interoperability, User Feedback, Conducting Pilots Cyber Security capabilities, Data Sovereignty, Data Security, Business Continuity Planning, Disaster Recovery, Natural Disaster event, Cyber Resilience testing, Service Support, Usage of AI in digital services are few things to consider. This will ensure Digital ID services are matured enough before wider rollout.
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	Phasing will give enough time for Digital ID Services to mature and be ready. Also, the recent Cyber-attacks have exposed vulnerabilities and more work is needed to mature cyber security posture before we roll out another major change.
27	Is the balance between voluntary use and the exceptions to voluntary use, right? Are any additional exceptions appropriate?	People with limited access to digital services, Cultural diversity and other regional communities' groups should be consulted and Digital ID provisions should be made appropriate to ensure these Australian communities are not disadvantaged
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	No, minimum standards should be followed by all
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	Yes
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	Yes
34	Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards	Digital ID system and Data Standard should be outcome based and technology agnostics and allow for innovation and technical advancements



Page # of guide	Question	Your response
	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?	When it comes to Digital Services, Consumer Data Rights (CDR) and Digital ID should all be in harmony. Consumer choice, data privacy, data control, interoperability, data security, and other CDR insights and learning should be incorporated into the development of Digital ID. All of these provisions should complement one another.



Thank You

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]