PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

10 October 2023

John Shepherd PSM

First Assistant Secretary, Digital ID Taskforce
Department of Finance
1 Canberra Avenue
Forrest ACT 2603

Our ref: MDR-P068-C001

Dear Mr Shepherd

MDR Security Submission to the Digital ID Bill 2023 Exposure Draft

Thank you for the opportunity to respond to the latest Digital ID Bill and Rules drafts. We have been involved with the national Digital Identity initiatives since 2021, and have noted a significant number of changes have been made since the last round of exposure drafts released for consultation by the previous Government. We previously authored a paper for ASPI[1] highlighting a number of issues that should be considered to ensure any future iterations of this scheme had the best chance of success, and are pleased to see that progress has been made in a number of areas, although challenges remain.

Firstly we note that a very large amount of complex material that has been released for consultation in a very short timescale – over 150 pages for the draft bill, 20+ pages of system rules and over 110 pages of accreditation rules, with only three weeks allowed for comments on the first two of these documents. We understand that Finance has held a number of closed-door roundtables and consultations with selected stakeholders in the lead up to this exposure draft, and is now keen to move forward with legislation as soon as possible. However, we suggest that a more comprehensive period of open, public, transparent consultation on such a major reform would be beneficial to draw upon the collective knowledge and input of all stakeholders and maximise the chances of broad public acceptance and uptake of the system.

In this submission we have provided our feedback so far, noting that our analysis is still at an early stage and ongoing. If the Department wishes to discuss further we would be happy to share more details at a appropriate date; we will also be presenting an update on our analysis at the Australian Information Security Association conference in Melbourne on 17th October.

Some high level observations thus far are:

- We note that the Trusted Digital Identity Framework (TDIF) is not mentioned anywhere. Although some portions of the TDIF requirements have been moved into the various documents, this is difficult to follow. Further clarity should be provided on the future of the TDIF and the mapping between the TDIF requirements and the new documents.
- The naming of the government's digital identity system as AGDIS is a welcome change from the previous proposal to just refer to it as "The Digital Identity System", which had potential to cause significant confusion and market distortion.

[1] https://www.aspi.org.au/report/future-digital-identity-australia

MDR SECURITY

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

- The clearer separation of the requirements into accreditation rules, participation rules and technical standards is welcome. However, we do have some concerns over both the use of the term "data standards" for the latter, as they go beyond what a data management professional might consider as data standards, into the realm of interface definitions, interoperability specifications etc. Also we have concerns over the operation of the Data Standards Chair, as such standards should ideally be developed and owned by the overall stakeholder community.

Responses to selected questions from the consultation guide are provided in the table below:

Page #	Question	Our 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?	The power to impose conditions is an important and potentially very valuable safeguard. We also note a formal role for the Regulator to be able to consult with the ACSC which is welcome. However, imposing special conditions on a specific entity should be a "last resort" power where the desired impact cannot be achieved by making common rules for all entities.
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?	Although the monetary penalties in this act are unlikely to be a significant deterrent for large corporations, we expect that for accredited entities it is the formal recognition of their status that provides the main incentive to comply. Therefore public disclosure and reprimands for non-compliance, along with a credible threat of suspension or revocation of accreditation could provide additional deterrent that will be more effective.
21	Are the additional privacy safeguards sufficiently robust, clear and practical?	The Bill contains a number of welcome provisions to improve the privacy by regulating the activities of accredited entities. However, it does not address the privacy risks from relying parties, who are not covered by the restrictions on data profiling, tracking and marketing that apply to accredited entities. Leaving this to be regulated by end user agreements and informed consent has not succeeded to date in taming the privacy impacts of technology companies. Such companies already build up and monetise massively detailed profiles on users. The digital identity system allows these to be tied to verified identities with the potential to be sold for even more.
21	Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited	We note the Act appears to ensure entities come under the Privacy Act regime which would mean that the recently increased penalties under that Act could

MDR SECURITY

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

Page #	Question	Our response
	entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?	apply as a further deterrent. As noted above, the deterrence value of public notification of breaches and potential revocation of accreditation may also have a greater impact than direct financial penalties.
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?	The private sector will expect certainty - not only on technical standards to be met, but also the commercial/charging mode will need to be clarified.
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	Factors for consideration include the maturity of private sector identity systems, including avoiding the AGDIS "crowding out" such systems; and also alternative options for interoperability with such systems. The Minister should also consider the ability of the AGDIS operating authority to scale, not only in terms of transaction throughput, but security and fraud monitoring and response.
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	The services market will need to have clarity on the proposed plans and timescales. The Government should aim for co-operating and interoperable private and public sector schemes. As noted above, care should be taken to ensure the AGDIS does not crowd out private sector systems. If AGDIS does become the dominant player in the market, further safeguards may be needed to protect other stakeholder interests.
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?	The voluntary principle is key to success of the digital identity scheme, so any exceptions should be limited. The circumstances in which the regulator can grant such an exemption should be clearly defined and limited.
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	The interoperability principle is key to success of the digital identity scheme. Further clarification should be provided on the exemption for "promoting the use of digital IDs", as this may create a perceived conflict with the voluntary principle.
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	See above comments on the privacy risks from relying parties. While the reasons why such parties are not subject to an accreditation regime are understood, the participation rules may provide an opportunity to limit some of worst potential for harm.
34	Noting the pace of technological change and the need for Digital IDs to stay	The Data Standards Chair should operate through a broad consultative approach to ensure the buy-in of all stakeholders to the standards that they set. This will

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

Page #	Question	Our response
	protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?	ensure the right balance between keeping standards up to date against the reasonable timescale expectations for accredited entities to make required adjustments.
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?	The Data Standards Chair model requires further clarification: - The name is potentially misleading as this role has power to set not only "data standards" but technical and interoperability standards - As a fixed term statutory appointment, the chair has significant power to mandate technical standards without commensurate accountability. There appear to be only very limited obligations to consult and seek consensus, yet such an approach should be routine for technical standard setting. Also, once appointed the chair can only be removed in limited circumstances. - The clause specifically permitting the chair to use consultants appears unusual – why does this need to be specifically legislated? - The rights for the chair to arbitrarily set their own terms and conditions to engage such consultants appears strange. Does this mean that such services could be procured without regard to Commonwealth procurement rules, and/or that normal conflict of interest safeguards may not apply to such procurement of services?

Yours sincerely

Rajiv Shah