PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

19 January 2024

Senate Standing Committees on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

Our ref: MDR-P068-C003

Dear Sir

MDR Security Submission to the inquiry into the bills of Digital ID Bill 2023 & Digital ID (Transitional and Consequential Provisions) Bill 2023.

Thank you for the opportunity to make a submission to your inquiry. We have been involved with the national Digital Identity initiatives since 2021, and have noted a significant number of changes and improvements in the proposed plan as it has evolved. 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. We have also presented on the current state of digital identity in Australia, the future direction and potential challenges at the Australian Information Security Association national conference in October 2023, and provided a previous submission to the consultation on the exposure drafts issued by the Department of Finance a few months back[2].

While we are pleased to see changes that address many of the points raised in that submission, some comments and recommendations still stand. Further review of the updated proposed drafts and accompanying documents has raised additional issues that are discussed below. However, time and resource constraints have limited the depth and breadth of our review, hence these should not be taken as a comprehensive review or commentary on the proposed legislation.

We would welcome the opportunity to discuss any or all of these issues further if that would be of assistance to the committee's work.

Level of public engagement and unrealistic review timescales

As we noted in our submission to the Department of Finance's consultation on the exposure draft of the Digital ID Bill, very little time has been allowed for consultation and review with the public on the details of the proposed legislation and related instruments. For the exposure draft in September 2023, almost 300 pages of material (over 150 pages for the draft bill, 20+ pages of system rules and over 110 pages of accreditation rules) was issued with only three weeks allowed for comments on the main bill. This time around, in the run-up to Christmas over 500 pages of material (in the form of two bills and accompany Explanatory Memoranda) were released, with submissions to your inquiry due in mid-January, still in the traditional summer holiday season. Unless organisations had existing connections with the project that allowed them early visibility of the materials, or at least pre-warning of their release, or they are

[1] https://www.aspi.org.au/report/future-digital-identity-australia
[2] https://www.digitalidentity.gov.au/sites/default/files/2023-11/mdr_security.pdf

MDR SECURITY

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

large organisations with significant resources that can be mobilized at short notice, this process does not allow for them to meaningfully engage with the process.

The impact paper included in the explanatory memorandum to the Digital ID Bill actually notes[3]:

An inherent constraint upon any government action in digital ID is the complexity of this subject matter and the low familiarity and exposure of the community to this concept and AGDIS to date. This apparent low level of public understanding could lead to any Australian Government regulation in this area to be misconstrued or viewed with hesitation and distrust.

Hence it is perplexing that the Government now appears to be rushing through the consultation process without allowing proper engagement with all stakeholders, not just a privileged few with the right connections and/or resources.

Recommendation 1: 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.

Transparency over potential influence and lobbying

The impact paper included in the explanatory memorandum sets out a detailed history of the consultations on this subject going back to 2016. However, it appears to have a "black hole" from September 2021 to September 2023. This was a period which saw a change of Government, transfer of responsibility for the project to the Department of Finance, and a significant rewrite of the legislation from the previous exposure draft. Previous commentary has suggested this was done in consultation with a range of stakeholders, but there appears to be a lack of transparency over who has had the opportunity to influence the legislation over this two year period (especially noting the subsequent very compressed timetable for true "public consultation" since October 2023 noted above). This could lead to concerns about undue influence from narrow segments such as multi-national companies with sufficient resources to lobby ministers and officials. This raises doubts whether the outcome is fully in the interests of the Australian public, and if it provides the right opportunities for sovereign industry capability to be part of the delivering the required capabilities. Problems of "regulatory capture" by multinationals on related technology fields that emerged a decade or more ago are only now being addressed (see for example the commendable work of the eSafety commissioner over the last 12 months or so). In the case of digital ID these should be addressed at the outset to ensure a balanced outcome.

Recommendation 2: There should be full disclosure of all meetings held by any commercial organisations with the Minister's office and/or the Digital ID Taskforce where plans for Digital ID were discussed. This required to build confidence in the lengthy process that has been conducted behind closed doors to bring this legislation forward, before a very compressed and rushed public consultation. There should also be full disclosure of any consulting engagements or other contracted assistance used to develop policy options, proposals and legislative drafting.

[3] Digital ID Bill 2023 – Explanatory Memorandum, page 200

MDR SECURITY

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

Unrealistic cost benefit calculation and assumptions

The assumptions used in the cost-benefit analysis presented in the impact paper appear to be unrealistic, and the calculation method does not appear to be appropriate.

For example, the benefits appear to have been calculated[4] using the *current* number of annual transactions using the digital ID system (myGovID) and assuming a saving of 115 minutes per transaction. However, from our own experience, many of our current transactions using myGovID are already much quicker than 115 minutes (a testament to the utility of the current system!), and some take as few as 2-3 minutes. Therefore, it is highly unlikely that a saving of 115 minutes could be achieved for all current transactions. It is possible the basis of estimate is an expectation that the current volume of transactions would double as a result of the proposed option – but then this assumption should be stated. Even then, we would contend that it is unlikely that 115 minutes can be saved on each and every transaction that moves to using myGovID - for example, time is saved when first setting up an account to manage company taxes online, which might be of order 115 minutes, but then the time taken for each use of the system to lodge a quarterly return is more dependent on the ATO's systems for filling and submitting data, and already takes less than 115 minutes even using current alternatives. On the other hand, although apparently flawed, the benefit calculation may be a gross underestimate. The analysis does note that it completely ignores any benefits of enabling broader digital economy transactions in the private sector. Other research[5] has estimated digital identity could unlock up to $11bn per year in economic value.

On the other side, the cost impact on regulated entities appears to be underestimated – for example for accredited participating entities, it appears the costs per accredited entity are estimated as approx. $30.8k for initial application and $12.8k per year ongoing costs[6]. However, a review of the draft Digital ID rules published in September 2023 shows that, for example, accredited entities will require a privacy assessment, protective security assessment, fraud risk assessment, technical assessment and testing of systems. At least some of these must be conducted by an external organization, and most will be required not only on application but to be updated at least every two years. Given that, in our experience, a single independent assessment on one aspect such as privacy, conducted by external consultants, would cost well over $30k, we suggest it is unlikely that total compliance costs on external suppliers will be as low currently assumed, even before adding in the costs for an entity's own internal resources.

Although it is possible, or even highly likely, that there is a compelling cost-benefit case for putting in place a legislated accreditation scheme and to underpin the AGDIS, a case based on inappropriate calculations does not form a sound basis for ongoing management and tracking of costs and benefits through the implementation phase. Furthermore, entities considering accreditation and applying for participation in the AGDIS should be given realistic estimates to rely upon for their own internal business cases.

---

[4] Digital ID Bill 2023, Explanatory Memorandum - page 247
[5] Australia Post Digital Identity White Paper (auspost.com.au)
[6] Explanatory Memorandum – Digital Identity Bill 2023, pages 314-317, calculation based on Tables 16 & 19

MDR SECURITY

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

Recommendation 3: A realistic estimate of costs and benefits should be prepared that confirms the net positive impact of the proposed initiatives, and a set of realistic assumptions that can be tracked and managed through implementation.

Role of the Digital Standards Chair

Firstly, we note the term "data standards" may not be appropriate, as the responsibilities of this role go well beyond what a data management professional might consider as data standards, into the realm of interface definitions, interoperability specifications etc.

More generally, 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.

As a fixed term statutory appointment, the chair has significant power to mandate technical standards without commensurate accountability. 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 ensure the right balance between keeping standards up to date against the reasonable timescale expectations for accredited entities to make required adjustments. There appear to be only very limited obligations to consult and seek consensus – for example submissions should be solicited, but need only be considered "if the Chair considers it appropriate to do so" – effectively allowing an arbitrary refusal to consider submissions.

Recommendation 4: The Data Standards Chair should have clearer obligations to consult broadly, to actually ensure that submissions are considered in detail, and priority is given to building stakeholder consensus.

We note that proposed clauses in the exposure draft to give the Data Standards Chair a specific right to use consultants, and an arbitrary right to set the terms of engaging such consultants that could potentially bypass Commonwealth Procurement Rules and checks on conflicts of interest have been dropped. However, this change seems to have been made without being noted by the Department[7], and the rationale for why such unusual provisions were originally included in the exposure draft is unclear. Better transparency around this would help to provide confidence that the drafting of the bill.

Recommendation 5: To ensure transparency and confidence in the legislation drafting process, the rationale should be provided by the Department for originally including clauses on use of consultants by the Data Standards Chair in the exposure draft, and the subsequent decision to drop these.

Digital ID Rules

Although not tabled as part of the legislation under review, the Digital ID Rules are effectively incorporated by reference. Based on the exposure drafts provided by the Department of Finance in October 2023, these are a significant instrument – over 100 pages containing highly complex, specific technical requirements. They specify what assessments need to be provided when applying for accreditation, details about what these assessments must contain, and then go into technical details such as precise accuracy rates required for algorithms used and even the number of bits of entropy used in cryptographic primitives. While it is right that such detail should not be in the formal legislation, an updated draft has not been provided when legislation is tabled. This may raise concerns, especially

[7] https://www.digitalidentity.gov.au/legislation#:~:text=Amendments%20to%20the%20legislation

MDR SECURITY

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

given that the Transitional Provisions Bill removes any requirement to consult on changes to these rules, or any ability for Parliament to disallow such changes, in the first six months after Royal Assent.

Recommendation 6: The proposed initial version of the Digital Rules should be tabled for before the final reading of the bills; and the obligations for consultation and potential disallowance of changes be reconsidered for the initial transition period.

When drafting such complex technical rules, a balance needs to be struck. Using contemporary best practice can ensure the system will incorporate strong security and privacy protections. However, it should be ensured that the requirements are not so prescriptive that potentially only one vendor's products and services are able to comply. This will minimise procurement, probity and supply chain risks. The Digital ID Bill should seek to stimulate competition and encourage development of sovereign industry capabilities as part of our digital economy. We have noted above a lack of transparency over who may have had the opportunity to influence a highly technical level of detail that may be only understood by a small number of people. Can we be confident that the right balance has been struck?

Recommendation 7: A truly vendor-independent technical review should be conducted of the Digital ID Rules (if this has not been conducted to date) and the results published.

Privacy

The Bill contains several 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.

Recommendation 8: Improved privacy protections should be legislated for personal data that relying parties obtain from an accredited entity and/or the Australian Government Digital Identity System.

Clarity of drafting and mandatory requirements

As noted above, our preparation of this submission has been severely impacted by time and resource constraints; also we are not legally qualified and so offer only a layman's perspective on the bill drafting. However, we have noted some examples where the explanatory memorandum appears to create confusion on whether certain requirements are mandated. For example:

1. Page 25, paragraph 68 of the Explanatory Memorandum suggests it is a matter for the entity whether to provide the listed documents and information required for the Regulator to make a decision on approval of the application; however the latest available draft of the Digital ID Rules (see for example Clause 2.2) states "an application for accreditation must be accompanied by" such documents, so the government's intent does appear to be to mandate such assessments to be prepared and submitted.
2. In the Digital ID (Transitional and Consequential Provisions) Bill 2023, part 3, it states that a "condition" for the listed entities to be approved to participate in the Australian Government Digital ID System is to "directly connect to the entity referred to in column 1 of item 3" (the Services Australia digital identity exchange). However, paragraph 27 of the accompanying Explanatory Memorandum states this does not prevent an entity from connecting to another

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

participant – so the approval is not actually conditional on directly connecting to the Services Australia digital identity exchange?

Recommendation 9: The legislation drafting is reviewed to ensure clarity on what requirements are mandated and which are optional/recommended only.

Yours sincerely

Rajiv Shah