PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

25 June 2024

John Shepherd PSM

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

Our ref: MDR-P068-C007

Dear Mr Shepherd

MDR Security Submission to the Digital ID Rules, Accreditation Rules and Data Standards Consultation

Thank you for the opportunity to respond to the drafts of the Digital ID Rules, Accreditation Rules and Data Standards. However, due to a lack of awareness of the consultation, we regret that we are unable to provide an appropriately detailed and considered submission. Although according to the digitalidentity.gov.au website, this consultation opened on 28 May, it was only announced on the Department of Finance website on 17 June 2024, with submissions due by 25 June 2024. Although MDR Security has taken the time and effort to provide submissions to your previous consultations, we were not sent any notification of this new consultation being underway, and hence only became aware of this a few days ago. Given other pressures at the busy end of financial year period, we have only been able to allocate limited resources to respond before your deadline.

While it may be unfortunate co-incidence, we note previous consultations in October 2023, and via a Senate inquiry in January 2024 were also challenging for those not in your "inner circle" to respond to, due to a lack of advice notice, large volumes of documentation to review and very short timescales to respond.

MDR Security is very supportive in principle of the need for a Government backed digital identity scheme in Australia, and indeed championed it as an appropriate part of the response to major data breaches such as Optus in 2022. We believe your proposed federated trust model, building upon the previous TDIF experience, is the appropriate approach. We have invested significant time and effort in reviewing many hundreds of pages of documentation that you have issued for consultation in the past, and where we do not agree with some of the proposals, have aimed to provide constructive feedback and suggestions as to alternatives. As examples, we would refer to our submission to the October 2023 consultation, and to the Senate Inquiry in January 2024. If you would be interested to hear more details about our research and feedback, we would welcome the opportunity to meet with you and discuss this.

In the meantime, given your compressed timescales and lack of notification, we provide just a couple of high level selected comments for your consideration.

1. We remain concerned about the construct of the Data Standards and the role of the Data Standards chair. The Chair will be appointed by the Finance Minister for a term of up to 3 years with very limited provisions to allow early termination of the appointment. The Chair has unfettered power to dictate the contents of the Data Standards, which will then have legal force. While the Act has some

MDR SECURITY

PO Box 248
Deakin West
ACT 2600

info@mdrsecurity.com.au

obligations for the Chair to seek in put it provides no requirement to consider such input. Also noting the approach taken to public consultation to date, it is not clear that meaningful opportunities for public consultation would actually occur in practice. Having technical standards effectively set by bureaucratic diktat is unusual in the technology world - co-design and ownership across all stakeholders is more common. As an alternate model to consider, in Canada the detailed framework for digital identification and authentication is being developed by the Digital Identification and Authentication Council of Canada, known as the DIACC, is a non-profit coalition of public and private sector leaders. In other areas of technology, such as AI and quantum, the Government has explicitly called for an industry-led approach to standards.

2. The cyber security requirements are vital to ensuring confidence in the system. We note that the various documents contain a range of requirements in different places, but these do not appear to provide a coherent end-to-end security assurance regime. For example, the governance regimes suggest a choice between ISO27001, the PSPF or an equivalent regime, but the Essential 8 seems to then get added into the mix, even though ACSC's own guidance suggests the Essential 8 is not really suitable for large distributed data platforms. Also, on the technical requirements there is a patchwork of very specific "hot buttons"; not only do these not actually cover all potential risks, but it is not clear which have clear technical merit, and which may simply have the effect of artificially limiting the choice of products that could be used in implementation. We would recommend a full end-to-end threat model and plan of controls, perhaps structured in line with the NIST framework (discover, protect, monitor, respond and recover) to ensure coverage across the full security lifecycle. We have conducted some more detailed analysis that could support such an approach, and would be happy to discuss findings so far, but have been unable to provide it here due to the time constraints.
3. We regret we are unable to respond to most of your detailed consultation questions in the time available but specifically in response to your question on Clause 3.8 (Penetration testing requirements) we do not believe the changes are particularly helpful or relevant in addressing the core issues. From our experience, there is a risk that a poorly scoped penetration test results in the tester spending a fixed time window trying random techniques and attack paths, resulting in a random list of observations and suggestions unrelated to the actual risk profile of the deployed system. Also, the option for the cloud service provider to simply have carried out the types of generic testing listed in subclause (2) appears to allow for a complete lack of testing of the details of how the accredited entity has actually implemented their solution on this cloud infrastructure. We suggest penetration testing should be linked to threat modelling of the overall system, and test at the application as well as infrastructure layers of the architecture.

Please do not hesitate to contact us if you have any questions or would like to discuss any of the matters in this submission or our previous submissions. As noted above, we regret that due to only becoming aware of this consultation round at a late stage at a busy time of year we have been unable a fully detailed and considered response by your specified deadline.

Yours sincerely

Rajiv Shah