From:
Willyama Services Pty Ltd
Level 1, 6/12 Albany Street
Fyshwick ACT 2609

To:
Digital Transformation Agency

Concerning:
Invitation to provide submissions and feedback to the DTA on their June 2021 Digital Identity Legislation Position Paper.

In accordance with invitation to contribute as presented in the DTAs Digital Identity Bill position paper, the following pages provide questions are proffered for the DTAs consideration and explanation.

Yours Sincerely
Michael Knight
Enterprise Business Architect.

Question 1 – Interactions with inter-dependent Australian Government Agencies.

Assuming that the resources for the **Trusted Digital Identity** (TDI) capability's governance and oversight functions are being relocated as a portfolio into the **Department of Prime Minister and Cabinet,** what is the answer to the following question.

> **Is it a DTA requirement to ensure that the the TDI when considering the Digital Identity Bill (the Bill) the exhibits the same public trust and transparency, allocated to the proposed Digital Identity Bill by conducting a Privacy Impact Assessment on the proposed Bill?**
>
> **This assessment would parallel the precedent set by PM&Cs Office of the National Data Commissioner for a very similar proposed legal instrument namely the Data Availability and Transparency Bill. (see ONDCs URLs below)**

To further clarify the question – and avoid ANY opaque "maybe" style of answer:

> **If the answer to the above question is "no", why would a PIA for the proposed Bill not be necessary?**
>
> **If the answer to the question is "yes", when would you anticipate that the PIA be scheduled and when will the results of the PIA be published?**

FYI - A copy of the Data Availability and Transparency Bill PIA can be found at https://www.datacommissioner.gov.au/resources/2021-privacy-impact-assessment via https://www.datacommissioner.gov.au/ .

Question 2. Concerning the rights of states and territories

This matter appears to be treated within the position paper with the Australian Government assuming a role of dominance.

How will the Bill and TDIF harmonise relationships with state and territory privacy and consumer rights frameworks?

Question 3. On the specific differences between the DTAs interpretation of the terms Guidance and MUST.

The **Trusted Digital Identity Framework** (TDIF) glossary defines the term MUST, MUST NOT and MAY in a context generally understood by generations of Australian Government entities.

The term MUST is also defined at the beginning of all TDIF documents accordingly:

"MUST. *Means an absolute requirement of the TDIF. Failure to meet this requirement will impact the Applicant's ability to achieve and maintain TDIF accreditation. Source: TDIF.*
MUST NOT. *Means an absolute prohibition of the TDIF. Failure to prevent this prohibition from occurring will impact the Applicant's ability to achieve and maintain TDIF accreditation. Source: TDIF.*
MAY. *Means truly optional. This requirement has no impact on an Applicant's ability to achieve or maintain TDIF accreditation if it is implemented or ignored. Source: TDIF"*

How does the DTA reconcile their direction that the TDIF is "guidance" when every clause in TDIF #04 v1.3 is individually marked either MUST or MUST NOT?

Will the TDIF be incorporated into the Bill in a manner similar to Schedules One and Two of the Privacy Act?

Question 4. The ability of the Bill to reference objective measurements.

The TDIF is written in lawyer type “legalese” and uses terms that cannot be objectively quantified by ICT Enterprise Architects for the purposes of developing a solution that satisfies the stakeholders business needs.

An example of this mis-interpretable “legalese” is the use of the terms “reasonable” and “unreasonable” – legal terms that are highly subjective and can only produce outcomes that are judgements by a reasonable person and cannot rely upon evidence in fact and opinion and cannot be objectively measured or quantified.

The following is an extract from TDIF #04.

"TDIF Req: PRIV-03-06-01; Updated: Mar-20; Applicability: A, C, I, X
The Applicant MUST only collect Personal information that it is permitted to collect under law and that is ***reasonably necessary*** *for one or more of its functions or activities directly relating to identity verification."*

> **How does the DTA intend the Applicant/Participant as executor of the TDIF in its own context establish a common baseline regarding operations when there are very few objectively defined measures?**

The argument that is entertained here is that the wording of the TDIF is highly interpretable and has the ingredients that can be combined to sustain a healthy lawyers breakfast.

It could be strongly suggested that whilst any argument concerning this perspective will not constrain the larger private entities that can provide the funding to pursue their particular perspective via a legal stoush, Australian SMEs are somewhat less well-resourced and therefore the SMEs ability to accept the risk and change presented by the TDIF are much weaker.

Question 5. Contrarianism

TDIF #04 mentions the following regarding the PSPF and ISM:

> *" To the extent of conflict between:*
> *• Any requirement in these TDIF protective security requirements and the current edition of the PSPF, then the PSPF takes precedence.*
> *• Any requirement listed in these TDIF protective security requirements and the current edition of the ISM, then the ISM takes precedence."*

> *"**TDIF Req: PROT-04-02-21; Updated: Mar-20; Applicability: A, C, I, X***
> *The Applicant MUST have in place secure measures during all stages of ICT systems development. This includes certifying and accrediting ICT systems in accordance with the ISM (or a similar process for non-government Applicants) when implemented into the operational environment."*

Clearly, the latest revision of the TDIF #04 has recognised the correct order of the PSPF and the ISM, recognising the PSPF provides Government policy and the ISM provides advice or guidance that clarifies the requirements of the PSPF.

The first dilemma is that TDIF **PROT-04-02-21** uses the term "**secure measures**" – which are neither defined nor objectively described and therefore need to be quantified. And the clause then states "**or similar process for non-government Applicants**".

Validation of these two different security perspectives will be highly subjective - since the harmonisation of different entities perspectives may require an appropriate legal instrument and a derivative well defined objective framework.

The second dilemma is the misunderstanding by the DTAs TDIF authors that Australian Government ICT Systems are not certified or accredited in accordance with the ISM. The ISM provides guidance (24 times) and advice (17 times).

And at the OFFICIAL and OFFICIAL:SENSITIVE security categorisation levels, self-assessment but not IRAP assessment by Australian Government entities is not a requirement.

The DTAs Digital Identity Bill position paper clearly describes the function of the **"Oversight Authority"** (130 times) in providing governance over the accredited capability although there seems to be some confusion in the appointment of an "Oversight Authority" and an "Information Commissioner" [Fig. 9] , and the of definition an "independent statutory officeholder" and a "statutory officeholder" as the appointed "regulator" [p. 61].

Noting that the PSPF is not law:

When can the DTA clarify the TDIF in the context of the PSPF and eliminate interpretations that will increase costs to the private sector?

Question 7.- Annual reviews and the participants character test.

Suppose an entity has accreditation to perform other similar or related services for the Australian Government from an associated entity (ACIC et. al.).

From a governance perspective these entities are probably required to receive annual reports for these services.

The questions concerning the character test are twofold :-

> **Firstly, should it be a requirement to register these other services and provide copies of these annual service reviews/reports to the "Oversight Authority"?**

(I do note that there may be restrictions on reporting content - but this matter only concerns reporting the submission of reports if content is restricted.)

> **Secondly, if an entity fails to satisfy any "compulsorily listed" Australian Government reporting or reviewing requirement , would it be within the "Oversight Authority's" scope to issue a "show cause" notice to the Participant as to why their accreditation should continue?**

Question 8. TDIF Referencing

The latest revision of the TDIF documents shows a marked evolution of the DTAs understanding of the Australian Governments requirements.

However, the documentation continues to confuse the reader by severely limiting its sources of reference and truth.

When can the DTA provide a properly referenced TDIF?

The oversight and quality of the current documentation leaves a lot to be concerned about.