TELSTRA CORPORATION LIMITED

Digital Transformation Agency

Digital Identity Legislation – Exposure Draft

Public submission

27 October 2021

CONTENTS

EXECUTIVE SUMMARY

Telstra welcomes the opportunity to respond to the Digital Transformation Agency's (**DTA's**) exposure draft of the Digital Identity (**DI**) legislation. The Trusted Digital Identity System (**TDI system**) is a key component of the government's Digital Economy Strategy and we have noted in previous submissions the criticality of trust, from both participating entities and users of the system, in the success of the TDI system. To this end, we appreciate the considerable effort and level of detail invested in the development of the exposure draft of the DI legislation, and we commend the DTA on a robust draft Bill that enshrines privacy, security, fraud prevention, and user experience and inclusion in the DI legislation.

Our submission comments on the following themes:

Liability. We are pleased to see the DTA acknowledge the need for entities to limit their liability for participation in the TDI system. However, there remain gaps relating to liability that require further consideration, and we recommend introducing caps on liability and extending the protection from liability to relying parties. We also recommend the Bill is amended so it does not require absolute compliance with the Act to benefit from protection, liability for consequential loss is expressly excluded and the Commonwealth should bear appropriate liability for participating in the TDI system.

Affected parties. We recommend the explanatory statement clarifies "point of contact" and provide some examples of mechanisms that users of the TDI system can use to make contact with accredited entities. We also suggest some improvements to the procedures for accredited entities to notify the Oversight Authority (**OA**) of the inability to contact individuals and businesses affected by an incident that we consider will be both more efficacious for the OA and simpler and more effective for accredited entities to implement.

Reportable incidents. We propose greater alignment with the Notifiable Data Breach (**NDB**) scheme under the Privacy Act, both in terms of the thresholds for reporting and the timeframes within which reports must be provided.

Interaction with other legislation. We are concerned that the introduction of bespoke privacy obligations for digital identity information under the TDI system will lead to complexity not only for accredited entities to navigate, but also for consumers to understand their rights. As such, we recommend closer alignment to the Privacy Act, where possible, as well as other relevant legislation in the health sector such as the Healthcare Identifiers Act 2010. We also note a potential for multiple penalties to be applied where the subject matter of the DI legislation overlaps with other legislation. We recommend the DTA clarify that civil penalties cannot be imposed multiple times under different legislation for the same conduct.

Following these four major themes, our submission addresses a handful of other matters, including requests for the DTA to provide clarity on the relationship between Key Positions and individuals within an accredited entity, clarification on notice periods, compliance assessments, publication of an accredited entity's privacy policy, amongst other things. Our submission concludes with a brief list of terminology we consider will benefit from clarification.

01 Introduction

Telstra welcomes the opportunity to respond to the DTA's exposure draft of the DI legislation. We appreciate the considerable effort and level of detail invested in the development of the exposure draft of the DI legislation, and we commend the DTA on a robust draft Bill that enshrines privacy, security, fraud prevention, and user experience and inclusion in the DI legislation. Our submission provides feedback to the DTA on matters we consider would benefit from additional clarity either in the instrument or in the explanatory note that accompanies the instrument. Our recommendations focus on matters we consider would assist with the commercial viability and uptake of the TDI System while balancing the trust and security requirements of the overall framework.

Our submission represents the entire group of Telstra companies, including Telstra Health and Telstra Purple, and we consider this breadth gives us a unique and deep insight into the value, and values, of the digital economy. The commentary we provide in our submission draws on our own experience developing a trusted commercial ecosystem in the rapidly evolving digital landscape of today's technology industry.

In this submission, we use the following terminology:

- **Bill** – refers to the exposure draft of the *Trusted Digital Identity Bill 2021* (in some instances we refer to it as "**the Act**", referring to a future point in time where the Bill has received royal assent);
- **Accreditation Rules** – refers to the draft of the *Trusted Digital Identity Framework Accreditation Rules 202x*;
- **TDI Rules** – refers to the draft of the *Trusted Digital Identity Rules 20xx*;
- **DI legislation** – refers to any or all of the above; and
- **Explanatory Note** - refers to the plain language explanatory memorandum that accompanies a bill submitted to the Senate.

Our submission is structured as follows:

- Section 02 contains our views on the liability framework, the dispute resolution framework and insurance requirements;
- Section 03 considers two matters related to users who may be affected by an incident;
- Section 04 looks at reportable incidents in relation to the thresholds for reportable incidents and the timing wherein accredited entities must notify the OA;
- Section 05 considers matters related to the likely interaction between the Bill and existing legislation, most notably the Privacy Act;
- Section 06 contains a number of minor matters for the DTA's consideration; and
- Section 07 contains a list of terms used throughout the proposed legislation we consider would benefit from clarification and some typographical errors we have identified.

02 Liability framework

2.1. Limitations on liability

As identified in our response to the Position Paper, there are inherent risks in any identity system and it will be critical to industry uptake that there is appropriate allocation and sharing of risk. We were pleased to see

section 39 of the Bill acknowledges the need for entities to limit their liability for participation in the TDI system. However, there remain a number of gaps relating to liability that require further consideration. We have set out our recommendations below.

- ***The protection from liability under section 39 of the Bill should extend to liability to end users and the Government.*** The protection afforded by section 39 only applies to limit liability of an accredited entity to another accredited entity or to a participating relying party. A lack of protection from liability to end users or the Government places a disproportionate regulatory burden on accredited entities to absorb potential loss. It is also inconsistent with the principle that accredited entities should not be liable under the TDI system if they have complied with their obligations. We recommend section 39 of the Bill be amended so accredited entities are also protected from claims by end users or the Government.
- ***The statutory contract regime should clearly link to the protection from liability in section 39.*** There is uncertainty in the Bill about whether the statutory contract regime in section 40 is subject to the limitation of liability under section 39. While section 40(5) provides scope for the TDI rules to prescribe limits on compensation an accredited entity must pay under section 40(4)(b), we don't believe this addresses the issue. We recommend the application of section 39 to statutory contracts under section 40, be expressly addressed in the Bill to avoid confusion.
- ***The protection from liability under section 39 should be redrafted so it does not require absolute compliance with the Act to benefit from protection.*** To benefit from the protection from liability in section 39, the Bill requires absolute compliance with the Act. This ignores causation and does not consider proportionality between the compliance failure and loss suffered. It also unreasonably narrows the protection afforded by section 39, as absolute compliance with the Act would presumably result in low risk of actual loss arising. In addition, the proposed TDI system is complex and could result in unlimited loss because of trivial or unrelated breaches of the Act, technical standards or even service levels determined by the OA. This does not reflect market practice. We recommend accredited entities be protected from liability where they have acted in good faith and the failure to comply with the Act is minor or did not cause the issue that gave rise to liability.
- ***Liability caps should be introduced to limit an accredited entity's liability.*** The statutory contract regime has potential for an accredited entity to be contractually bound to thousands of accredited entities and participating relying parties. Combined with the concerns outlined above, there is significant potential for financial exposure on an uncapped basis. We recommend each accredited entity's liability be capped under each statutory contract and an aggregate cap introduced across all statutory contracts. These caps could be tied to revenue or usage and we acknowledge they should not apply where an accredited entity has acted fraudulently, criminally or not in good faith.
- ***The Bill should expressly exclude any liability for consequential loss.*** The lack of exclusion for consequential loss does not reflect market practice. We recommend consequential loss be excluded for any accredited entities.
- ***The protection from liability under the Bill should extend to participating relying entities.*** Although participating relying parties will not take on as many responsibilities as accredited entities, a participating relying party may breach its obligations in a way that causes loss. We recommend the same principles limiting accredited entity liability under the Bill, including those proposed above, should apply equally to participating relying entities.
- ***The Commonwealth should bear appropriate liability for participating in the TDI system.*** It is reasonable for the OA to be immune from a damages claim in its role as a regulator. However, the Commonwealth should bear some liability for participation in the TDI system as the operator of the TDI system. Under section 152, the OA has no liability in the performance or exercise of any function or powers under the Act. This may absolve the OA from liability, even if it is acting as a participant in

the TDI system. It is not reasonable for the Commonwealth to be immune from liability whilst all risk is borne by participants. We recommend that the risk and liability positions under the Bill should apply equally across participants and Government in the TDI system, including any limitation on liability.

2.2. The TDI rules should codify the dispute resolution process upfront

While there is scope[1] for the TDI Rules to make dispute resolution provisions that need to be followed before an entity can apply for an order under section 40(3), the draft TDI Rules contain no dispute resolution procedures. A robust dispute resolution process is critical and should be codified upfront. Combined with greater clarity around a participant's liability position as we've recommended above, we believe this will lead to greater industry uptake. We consider existing industry based external dispute resolution schemes (such as the Telecommunications Industry Ombudsman) are unlikely to be appropriate. Instead, we consider the Office of the Australian Information Commissioner (**OAIC**), which already manages privacy-related complaints,[2] may be best placed to resolve disputes relating to the TDI system.

2.3. The Bill should provide clarity on insurance requirements

Section 41 of the Bill provides scope for the OA to require accredited entities to maintain adequate insurance against liability under the statutory contract regime. Given the current potential for broad, uncapped liability, it may not be possible for accredited entities to maintain adequate insurance to cover their potential liability. We recommend the Bill provide further clarity on the type, and value of, insurance cover that an accredited entity must have to be compliant. We also observe that some large corporations may elect to self-insure certain risks rather than maintain separate insurance policies, and we recommend the explanatory statement accompanying the Bill should clarify that "maintaining adequate insurance" could include self insurance of liability where that is appropriate in the context of the size and scale of the relevant organisation. We also observe cyber security insurance, particularly for large corporate entities, is difficult to obtain in the current cyber risk climate, meaning that some entities may struggle to comply with such a directive from the OA.

2.4. Clarification of suspended entities within the statutory contract

Under section 40(2) of the Bill, a statutory contract ends on the day on which approval is revoked, but it is unclear whether the suspension of an entity's licence would amount to revocation. We recommend that it be made clear in section 40(2) that the suspension of an entity's licence does not amount to revocation of approval and that the statutory contract continues during the period of suspension.

03 Affected parties

3.1. Point of contact for affected parties to seek information about an incident

Section 43(4)(a) of the Bill requires an accredited entity to "…*set up a point of contact to enable individuals to seek information and support about the occurrence, or suspected occurrence, of a digital identity fraud incident or a cyber security incident that has affected or may affect the individual(s)*".

We observe section 43 is not limited to accredited entities that have been accredited and onboarded, and therefore, extends to entities who have chosen to obtain accreditation but not onboard to the system. We

1 The Bill, section 42.

2 https://www.oaic.gov.au/privacy/privacy-complaints

understand this to be intentional and agree with the approach. We note from conversations with the DTA that "point of contact" is not intended to be limited to a natural person, and also refers to methods by which individuals may make contact with an accredited entity more generally. We support this approach, and suggest this be clarified in the explanatory note accompanying the Bill. For context, it is common in large corporations to use generic email addresses such as identitysupport@company.com.au as a point of contact rather than the name of an individual employee in the company (i.e., john.smith@company.com.au), or a range of other contact "mechanisms" for customers to contact the entity including webform(s) on internet pages (e.g., "contact us") or a function within an app.

3.2. Notification on inability to contact affected individuals or businesses

Section 43 of the Bill contains obligations on accredited entities in relation to either a Digital Identity Fraud Incident or a Cyber Security Incident. Section 43(2) requires accredited entities to "*make all reasonable efforts*" to contact individuals and businesses affected by the incident, and we support this "reasonable efforts" approach. Section 43(3) goes on to require an accredited entity to notify the OA within 7 days where the entity is unable to contact the individual or business concerned. We recommend the DTA should provide some clarification, most likely in the explanatory statement, on what qualifies as "unable to contact". For example, we would expect most contact of this nature to be made via email or postal address. Is a positive reply or acknowledgement from the affected party to the email or postal letter required to confirm that contact has been established? Alternatively, is the absence of the letter being returned, or in the case of an email, the absence of an automated "unknown address" response email sufficient to assume contact has been made?

We also have some concerns at the short 7 day period, commencing with the accredited entity "*becoming aware of the incident*" (section 43(3)) for the entity to notify the OA. Internal investigation into an incident to even identify which individuals may have been affected can take several days from first becoming aware of the incident, based on the scale, scope and complexity of the incident. We appreciate the DTA's policy objective is to keep the OA appraised of progress, and consider that a deliverable attached to a fixed point in time from the accredited entity first becoming aware of the incident may not achieve the DTA's policy objectives. If set too short, the entity may not have completed the analysis to identify affected parties, much less initiated contact. If set too long, the OA may not become aware of incidents in a sufficiently timely manner to be able to offer assistance. We recommend the clause is modified to require entities provide "all relevant information as soon as reasonably practicable". Further guidance could be included in the explanatory statement describing the type of information the OA requires, such as the number of individuals who have been identified as affected, and when an attempt(s) has been made to contact those individuals.

The comments above apply equally to section 44(3), which similarly requires a relying party to notify the OA within 7 days where it is unable to contact the individual or business concerned.

04 Reportable incidents and alignment with NDB scheme

Telstra recommends that the reportable incident obligations in the Bill align to the Privacy Act's NBD Scheme both in reporting thresholds and timing. The application of the NBD Scheme will allow entities to appropriately balance the need to inform individuals of data breaches while also allowing them to undertake incident investigations in a uniform manner.

4.1. Reporting Threshold

We fully support notifying participants when their data has been compromised or adversely impacted. However, the Bill sets a low threshold compared to the NDB Scheme for notification of an incident with

entities required to report even most minor incidents, regardless of the extent of impact. Reporting thresholds need to balance the opportunity for an individual to take timely mitigation action while also recognising that notifying an individual prior to investigation may mean unnecessary alarm. This will compromise the trust in the TDI system when an incident is contained or has minimal to no impact on the individual.

For this reason, we would strongly suggest aligning the threshold for reporting incidents to the NDB Scheme. The NDB scheme has been in effect for a number of years and carries the benefits of a sophisticated and integrated framework of supporting OAIC guides that define concepts such as unauthorised access, unauthorised disclosure or the likelihood of serious harm. The NBD scheme could be expanded to cover reportable incidents under the TDI system. It also has the benefit of giving accredited entities consistency of business operations, instead of creating complex and inconsistent regulatory obligations that could potentially apply to the same information.

We also consider that for this reason, the NDB scheme presents a cohesive opportunity to reduce regulatory complexity and the cost of operating the TDI system as it is likely digital identity information would be an Eligible Data Breach and therefore already be subject to reporting requirements.

We understand there may be benefits in requiring entities to notify any and all incidents with the potential to compromise the TDI system to the OA regardless of impact. If the DTA believes this is the case, we suggest a distinction be made between incidents that impact the TDI system and those that don't when requiring OA reporting.

We would strongly encourage the DTA to consider aligning the regime with the Privacy Act especially in relation to notification to affected individuals and businesses. This will stop unnecessary alarm being caused to those groups when there is minimal to no impact on them and will mitigate against notification fatigue. Pursuit of a niche set of reporting requirements for the TDI system also inevitably introduces cost to the new OA who will need to provide further clarity and regulatory guidance on new uncertain terms in the legislation including "significant probability", "compromised business operations" and when an attribute or credential is "unreliable" or "compromised". We also observe the OAIC has a privacy complaints facility, which we consider would be appropriate for managing DI related complaints (see our comments in section 2.2).

4.2. Timing of Reporting

As the DTA would appreciate, in a cyber security event, investigation is critical not only to understand the cause of the event but also to remedy and mitigate any adverse impact in a timely manner. Given the reporting threshold is so low for incidents and includes suspected incidents, the 24-hour timeframe for reporting to the OA makes it difficult for an organisation to undertake meaningful investigation to determine the extent and impact. It is highly unlikely that within 24 hours of becoming aware of a reportable incident, an entity would have much (if any) valuable information to provide the OA other than an incident appears to have occurred. Given the sensitive nature of the digital identity information, we agree that reportable incidents need to be notified to both the OA and impacted individuals in a timely manner. However, entities should be given a reasonable time period to investigate the incident (which could be quite short in some cases) allowing them to determine the impact (if any) and potential remedies.

As such, we recommend that the TDI Rules are amended from a strict '48 hour' rolling reporting requirement to instead require entities provide "all relevant information as soon as reasonably practicable". This would sufficiently meet the DTA's requirements for oversight of an incident while not requiring an entity to divert resources from investigating and resolving the problem to reporting on the problem.

We also provided comment on the 7-day notification to the OA on inability to contact individuals in section 3.2 of our submission.

05 Interaction with other legislation

5.1. Care not to overlap existing legislation

We appreciate the DTA's concerns about the sensitivity of the digital identity information. However, we are concerned that having different regulatory regimes for the same piece of personal information depending on how it is collected, will result in a very complicated regulatory framework not only for accredited entities to navigate, but also for consumers.

An organisation could be an APP Entity that is accredited under the Trusted Digital Identity Framework (**TDIF**), an accredited data recipient under the Consumer Data Right (**CDR**) energy regime, and an entity under the Healthcare Identifiers Act 2010 and My Health Records Act 2012. In undertaking its business activities, including as an accredited entity and under these regimes, it may collect the same type of personal information. However, it will be subject to different requirements on matters such as, whether consent is needed for use and disclosure to enforcement bodies or other third parties, the need to report data breaches to regulators and impacted individuals as well as destruction requirements. This will potentially result in entities having to create parallel, but different, privacy governance and compliance frameworks and may ultimately be a disincentive for accreditation. Consumers will also likely be confused as to why entities need their express consent to use or disclose their information under the TDIF, but do not have any similar obligation when the exact same information has been collected for other business functions. The different notification/reporting requirements (see section 4.1 of our submission) is also likely to cause consumers confusion and may inadvertently lead consumers to not take seriously NDB Scheme notifications, due to receiving notifications under the TDI Rules of incidents with minimal adverse impact on them.

In addition to potential overlap or discordance with the Privacy Act, the Authorised Uses proposed in Section 104 (and particularly 104 (f)) of the Exposure Draft has a significant overlap and potential contradiction with the Healthcare Identifiers Act 2010 and My Health Records Act 2012. Such inconsistency would be highly problematic for health and aged care providers and the health technology industry that supports them.

Note also that eligibility and use of identifiers for individual healthcare providers and healthcare provider organisations are also governed by the Healthcare Identifiers Act 2010. Section 11 (2) of the Exposure Draft calls out healthcare identifiers for individuals, but not for healthcare provider individuals. We recommend consideration of including healthcare provider individuals in the definition, noting the imperative to avoid duplication and additional compliance burden as set out in 6.1 of this submission.

We recommend the DTA seek to leverage existing privacy and health information laws to the greatest possible extent, rather than create bespoke obligations for the management of personal information under the TDI system.

5.2. Interaction with the Privacy Act

We understand the intention of the DTA is that the extension of the definition of "personal information" and the additional privacy safeguards in the Bill are only to apply to accredited entities when providing accredited services (i.e. when onboarded). The extension of the definition is not intended to apply to accredited entities (including onboarded entities) in relation to activities they perform *outside* of the TDIF. We recommend this distinction be made clearer. This is particularly relevant in sections 64, 76, 77 and 79 of the Bill, where their application is not clearly limited to the provision of accredited services.

5.3. Potential for dual penalties

The Bill[3] prescribes civil penalties for contravention of certain aspects of the legislation. However, the Bill does not state that civil penalties cannot be imposed twice for the same conduct, namely under this Bill and under another Act (for example, the Privacy Act).

We recommend the DTA clarify that civil penalties cannot be imposed multiple times under different legislation for the same conduct.

06 Other matters

This section of our submission contains major themes relevant to more than one aspect of the exposure draft of the legislation. In each case, we discuss our view on the possible problem we have identified and provide supporting evidence for the change in direction we recommend.

6.1. Potential to duplicate industry compliance burden in healthcare

Healthcare providers are connected to a growing number of services for patient and provider authentication, direct care provision, population and public health, and billing and administration. Technology providers in health (software applications and platforms) develop and maintain compliance with a number of technical and legislative regimes including technical, security and other physical compliance elements in order for healthcare providers to safely do business, and for consumers to securely access digital health services. This includes the Healthcare Identifiers Service, My Health Record, the National Cancer Screening Register, Services Australia, and MyGov. The cost to all health software providers and therefore all healthcare providers to maintain compliant technical connections to these services that are both secure and clinically safe is steadily increasing and has accelerated during the COVID-19 pandemic.

Noting that the technical standards for connection to the trusted digital identity systems may be made by the Oversight Authority (Section 36 of the Exposure Draft), strong consideration should be given to how standards and compliance regimes pertaining to existing technical infrastructure services and processes in health could be leveraged in order to reduce or eliminate any new technical compliance burden under the proposed Framework.

6.2. Clarity required on relationship between key positions and individuals

The Accreditation Rules defines a number of key positions, including Digital Identity Fraud Controller (DIFC), Chief Security Officer (CSO), Chief Privacy Officer (CPO) and Privacy Champion. We understand from our discussion with the DTA that a single individual, suitably qualified as required by the Accreditation Rules, may hold multiple key positions. For instance, an entity's Chief Technology Officer could also undertake the role of Digital Identity Fraud Controller if suitably qualified in fraud matters. We would recommend the Bill and/or explanatory statement is amended to make this clear.

We also note that the functions of the Privacy Officer and the Privacy Champion are quite broad in nature. While in smaller organisations it may be possible for a single individual to be responsible for all these functions, in larger organisations it is not unusual for these responsibilities to be spread out across a number of roles. This is to ensure these important activities are properly resourced by those with the specialist knowledge and skillset within each section of the organisation's business. Consequently, the ultimate responsibility for these activities may sit across different Executives within an organisation. We understand

3 Bill, Chapter 7, Part 3, Division 1, Section 119, p.104.

from our discussions with the DTA that it has no objection to the responsibilities for these privacy functions being spread across different roles. On this basis, we recommend the Accreditation Rules be amended to clarify that organisations have the flexibility to determine how best to manage these privacy requirements within their own internal structures.

6.3. Notice period to comply

The Bill contains obligations where an entity can be served a notice, and is required to comply with the notice within a "notice period". One example is section 25 of the Bill, which provides the OA with the ability to impose a new condition on an entity's approval to onboard to the trusted digital identity system, so long as the OA gives the entity a written notice in accordance with section (2). Under section (2)(b), the OA can "*request the entity to give the Oversight Authority, within the period specified in the notice, a written statement relating to the proposed condition*." A further example is section 126 of the Bill, which provides the OA with the ability to require an entity to undergo a compliance assessment, provided a written notice is provided.

The absence of guidance on the minimum notice period in these examples is in contrast to section 130 of the Bill (regarding the OA's power to require information or documents), where section 130(3) requires the notice period to be no shorter than 28 days.

We forsee the need to accommodate different minimum periods to accommodate different scenarios, and consider it impractical to prescribe a "one-size-fits-all" common mimum notice period in the legislation. Rather, we suggest the explanatory memorandum for the Bill (once one is developed) provide guidance to the OA on setting an appropriate duration for potential conditions that could reasonably foreseeably be imposed on entities. This will ensure consistency across similar situations, and will also set expectations for entities as to the duration they may expect for such situations.

6.4. Threshold for requiring a compliance assessment requires clarification

Section 126 of the Bill provides the OA the ability to require an entity to undergo a compliance assessment where it is satisfied any of the events in s.126(1)(b)(i)-(vi) have occurred or are suspected to have occurred. Subsections (iv)-(vi) are vague in the sense that terms such as "may have" and "material impact" are not defined.

We propose the explanatory memorandum for the Bill (once one is developed) provide guidance on what is intended by an incident that "may have" a material impact on the operation, and what the materiality threshold is. This will ensure consistency across similar situations, and will also set expectations for entities as to the duration they may expect for such situations.

6.5. Separate privacy policy for DI function

Section 3.2.2(1) of the TDIF Accreditation Rules requires an accredited entity to maintain a separate privacy policy for the entity's accredited facility and its other business or organisation functions. The Bill goes on to require that where an entity holds accreditation for multiple functions (e.g., identity service provider, attribute service provider or as an identity exchange), the entity is required to develop and maintain separate privacy policies for each kind of accredited facility, or where it has only a single privacy policy, it must maintain distinct sections addressing each of the entity's accredited facilities.[4]

[4] Accreditation Rules, section 3.2.2(2), notes (a) and (b). p.21.

While we appreciate the role of each kind of accredited function of an entity is different, we do not believe the content of a privacy policy will vary much across these different functions. Ultimately, the policy must comply with Australian Privacy Principles 1.3 and 1.4 and it should be up to the entity to determine how this is best achieved. We believe the proposed separate sections will lead to significant repetitiveness and unnecessary complexity within the privacy policy which will defeat the purpose of APP 1.3.

The DTA has not provided a justification for why separate sections in a privacy policy for an entity's different accredited functions would better meet APP 1 requirements. We recommend the DTA should either provide a justification to substantiate the need for section 3.2.2(2), or remove the requirement.

6.6. Law Enforcement Restriction

Section 81 prohibits the disclosure of digital identity information to enforcement bodies, unless an exception applies. A breach of this section will result in a penalty to the accredited entity. However, we note that some of the exceptions depend on what an agency "reasonably believes". We are unsure how an entity could satisfy itself of this. An accredited entity should not be liable for breaching this clause if they have, in good faith, relied upon representations made by an agency confirming the existence of the applicable conditions.

07 Terminology requiring clarification

We consider there are some terms in the Bill, Accreditation Rules and/or TDI Rules that would benefit from greater clarity to assist entities wishing to apply for accreditation to better understand the obligations of the legislation. This section contains the list of terms, along with our recommendation for how the definition may be improved.

Term	Reference	Suggested clarification
Cyber Security Incident	TDI Rules, section 4.	The term is defined as "*an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations*." • We recommend the explanatory note for the TDI rules provide guidance on terms such as "unwanted", "unexpected" and "significant probability". • We suggest the definition is expanded beyond just compromising "business operations" to include compromising the integrity of information within the TDI system, given *theft* or deliberate *manipulation* of information within the system may not compromise business operations per se, and may not yet amount to a fraud incident as defined in the term Digital Identity Fraud Incident.
Reasonable efforts	Bill, section 43(2), section 43(6), etc	There are a number of instances where phrases such as "reasonable efforts", "reasonable assistance", "reasonable grounds", etc. appear throughout the Bill. We suggest that each of these cases should be informed by guidance in the explanatory note. We note the Accreditation Rules, chapter 2 section 1.5(2) contains a description of "reasonable steps", and provides a list of "relevant matters" an entity should take into account, however, relevant matters to consider are not a the same as guidance on the steps that should be taken; they are examples of input considerations rather than output actions.