ANNEXURE 1

Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the Bill)
Comments on Exposure Draft

No	Issue description	Telstra commentary on practical implications	Telstra Recommendations
1.	**Liability for Undetected Breaches**	The Bill incorporates a concept that an entity is subject to the notification regime, even where it is not aware that a serious data breach has occurred – namely the obligation pursuant to s26WC(1) that an entity must notify where **"it ought reasonably to be aware"** that there are reasonable grounds to believe there has been a serious data breach. We anticipate that this language has likely been introduced to capture situations where an organisation is wilfully blind to a serious data breach. However, the inclusion of this language gives rise to some concerns on our part. Security incidents and complaints are generally raised within a large organisation such as ours through a number of channels (for example, directly to front of house, via an online webform, through social media etc). Some data breaches will also involve sophisticated security attacks. It may not be apparent that there is a serious data breach requiring notification until issues are ventilated either by multiple persons or via multiple channels. However, the language around 'ought reasonably to have been so aware' could give rise to a finding that the organisation ought reasonably to have been aware of an issue when just one complaint was lodged, rather than at the point that multiple complaints or channels pointed to a serious issue – with the potential for a finding that a data breach notification was not made 'as soon as practicable.' This could result either in organisations over-notifying (and creating concern where there is no good reason) or being unfairly targeted for not notifying early enough.	The concept of "ought reasonably to have become so aware" adds complexity to determining when to notify and to the application of the legislation. In our view, the concept should be removed and reliance should simply be placed on the question of whether an entity that is aware of an issue has sufficiently reasonable grounds to believe there has been a serious data breach. We note that organisations who have been wilfully blind may in any case be subject to potential penalties for a breach of the APP11 requirement that an entity take reasonable steps to protect personal information from unauthorised access or interference (implicit in which is an obligation to detect breaches).

No	Issue description	Telstra commentary on practical implications	Telstra Recommendations
2.	**Liability for Unconfirmed Breaches**	The Bill incorporates a concept that an entity is subject to the notification regime even where it is not sure that a serious data breach has occurred ie a view that there are **"reasonable grounds"** that a serious data breach has occurred is sufficient. We note our concerns that: a) What constitutes "reasonable grounds" will vary depending on the circumstances and could be determined retrospectively by the Commissioner; b) It is unclear whether the 'reasonable grounds' test is a 'reasonable person' test or one perhaps tailored to the complexity and resources of the entity in question; and c) There is no indication as to when the "reasonable awareness" should arise, for example – is a failure to have a certain standard tools and technologies that might allow for such reasonable awareness considered in this?	We would like to see further clarification and guidance provided on the threshold for reasonable awareness, either via changes to the Bill or in appropriate guidance notes. This should include guidance on the model minimum standard to which entities should be held accountable.
3	**Information Commissioner's Role**	Pursuant to s26WD(1), the Commissioner may mandate notification by an entity. Section s26WD(5) provides that an entity must comply with a mandated notification as soon as practicable after the direction is given. There is no equivalent in s26WD(1) to the provisions in s26WC(1) - which by virtue of s26WC(2) in effect define 'as soon as reasonably' practicable' as being within a 30 day timeframe. The effect of this is to give the Commissioner the power to mandate immediate notification without the entity having an opportunity to investigate the issue or have a right of reply to the Commissioner.	We appreciate from discussions with the Department that the mandated notification provisions were intended to be used only in limited situations involving a high degree of risk to a data subject. We understand and accept that in such very limited circumstances, immediate mandated notification may be appropriate. However, there is nothing in the wording of s26WD(1) that suggests the mandated notification right is limited to particularly high risk circumstances. The language for the most part simply mirrors the 'reasonable grounds' language in the s26WC(1) notification provision. We suggest that: • either the language of s26WD(1) be tightened to limit the kinds of situations where mandated notification can occur; or • if s26WD(1) is not tightened in the manner suggested, entities should be given some time to

No	Issue description	Telstra commentary on practical implications	Telstra Recommendations
			investigate the matter and respond to the Commissioner before immediate mandated notification is required. We also suggest that s26WD(1) be amended to make it clear that if an entity is not aware of a breach then the Commissioner should be under an obligation to provide the entity details of the alleged breach so that it may conduct its own investigation.
4	**Possession and/or control of data**	The Bill extends the obligation to notify to the entity that **"holds"** the relevant information that is subject to the serious data breach. In practice, more than one entity could "hold" information subject to the same data breach. This is because "hold" under the Privacy Act means having possession or control and therefore one party could be in possession and another in control. In a practical sense if a data breach is caused by a contractor in the possession of an entity's data but that data is in the control of the entity there may be conflicting requirements to notify. There is a significant risk of different messages going out for the same breach to the same individuals. Receipt of multiple notifications from separate sources could result in confusion and distress for impacted individuals and potential inconsistency in the message.	This section is likely to cause additional complexity and uncertainty. The existing OAIC Guidelines state that typically the organisation which has the direct relationship should notify including where the notification involved a third party service provider or contractor (ie the data controller). A similar clarification in the new legislation would be helpful.
5.	**An Ordinary Person**	The Bill introduces the concept of the **ordinary person**. The explanatory memorandum seeks to address this concept but it requires it to be read as part of the other relevant matters set out in the explanatory memorandum to gain proper definition. This is confusing and means the definition lacks clarity in any singular circumstance. For example, in any given incident the definition of the "ordinary person" may not revolve around the nature of the	Clarification around the concept of the ordinary person and the assessment of their role should be provided.

No	Issue description	Telstra commentary on practical implications	Telstra Recommendations
		recipient of the information or whether they are an ordinary person but rather lies in the assessment of the risk of that information being rendered intelligible (eg if there is a decryption key or if there are people available with the skills to convert it). Further, it is unclear whether the test of an ordinary person is a test for a reasonable expectation of technical ability or alternatively is it that person's ability to reconstruct the data through available services.	
6.	**Consequences**	The Bill provides that a failure to notify a breach is a breach of the Privacy Act. The Privacy Act itself provides for a number of circumstances which constitute a breach of the Privacy Act. Providing the additional breach offence for failure to report effectively constitutes a duplicate breach for the same incident. For example, APP 11 requires personal information to be held securely. A data breach that is not reported by an entity within the mandated time could result in a double breach/penalty under the Privacy Act ie failure to notify the breach and failure to adequately secure the data.	It should be made clear that in the event of a data breach the responsible entity is liable for a single offence under the Privacy Act.
7.	**Compliance Costs**	Compliance costs associated with the new legislation can be divided into 2 categories: 1) Establishing Compliance Systems The cost of establishing compliance systems is difficult to quantify up front particularly without the final terms of the legislation having been determined. 2) Ongoing Compliance costs These include both system and behavioural processes to raise potential privacy issues, streamlining the triage process and establishing metrics around these processes to allow monitoring and reporting.	Our experience in establishing similar compliance programs (for example the ACCC mandated SSU reporting) has proven this process to be both resource and time intensive. For larger organisations like ourselves with established compliance programs, the new reporting requirements can be implemented within existing frameworks. However, smaller organisations without the existing resources will no doubt incur more substantive compliance costs. The lower the complexity in the legislative requirements, the lower the costs associated with establishing the compliance systems and accordingly the ongoing compliance costs. We believe that addressing the concerns we have outlined in this submission will assist in minimising the associated compliance costs.