4 April 2018

COMMUNICATIONS ALLIANCE LTD
www.commsalliance.com.au

Mr Alan Marjan
Assistant Director
Critical Infrastructure Centre

Email: alan.marjan@homeaffairs.gov.au

Dear Alan,

RE: Feedback on TSS guidance material

Thank you for the information you provided at the recent stakeholder meeting (20 March 2018).

Communications Alliance welcomes the opportunity to summarise our feedback to the guidance material published at https://www.ag.gov.au/consultations/pages/Telecommunications-Sector-Security-Reforms.aspx. We hope our feedback assists the Critical Infrastructure Centre (CIC) to further develop the Telecommunications Security Sector (TSS) guidance material and to soon release an updated version of the Administrative Guidelines that accompany the *Telecommunications and Other Legislation Amendment Act 2017* (Act).

The following issues require further clarification to assist our industry with implementing and complying with a highly complex scheme.

Definition of material adverse effect

The Act stipulates that carriers and nominated carriage service providers (jointly: CSPs) must notify the Communications Access Co-ordinator (CAC) when they become aware that "the implementation [...] is likely to have a material adverse effect" in order to comply with the security obligation that the Act imposes on CSPs (314A(1)). Consequently, it is critical to understand when a change is likely to have such a material adverse effect. We acknowledge that this will often be a 'judgment call', given the imprecise nature of the language in the Act. It is unfortunate, nonetheless, that neither the *Fact Sheet Notification Requirement*, nor any of the other guidance documents provided so far, offer much assistance in this matter.

The *Fact Sheet Notification Requirement* appears to provide a nonsensical definition by stating that "A change is likely to have a material adverse effect if implementing that change may have an actual or measurable negative impact [...]" (emphasis added). How can an action be likely to have an effect if that action only may have a negative impact? Simplifying the sentence and replacing some words with synonyms, the sentence effectively reads: "A change is likely to have a negative effect if implementing that change may have a negative effect." Even replacing the 'may' with a more logical 'likely' still does not provide real assistance with the issue at hand.

In addition, it is not clear how a negative impact can be measurable without being actual. We suggest deleting the 'actual and' but note, as outlined above, that even once this definition has been amended to only use 'likely' and with the reference to 'actual' removed, it is questionable whether CSPs can derive much guidance from this definition.

Use of third party cloud services and offshore service providers

Slide 8 of the presentation used at the stakeholder information meeting on Tue, 20 March 2018 says that third party cloud services and/or service providers or facilities based outside Australia can be used provided that the information and networks using those services or facilities will be protected to at least the same standard as if those services were provided from within Australia.

As foreign governments typically have incursive powers to access information or facilities, it is by definition not possible to fulfil the security obligation to the same standard that could be applied in Australia. Even where offshore or cloud providers have been certified by the relevant Australian authorities, it is not possible to guarantee the same standard of protection.

The guidance presented at the stakeholder meeting is even more disturbing because it contradicts the statements made by the Attorney-General's Department (AGD) at the Parliamentary Joint Committee on Intelligence and Security (PJCIS) hearing on 23 March 2017. At that hearing, Mrs Chidgey, First Assistant Secretary, Cyber and Infrastructure Security Division, AGD, explained (when questioned on how the TSS framework addresses overseas assets and services) that CSPs' "obligations relate only to their networks and facilities to the extent that they have access and control. Where a communication is transmitted across infrastructure of an Australian provider and then on to a foreign provider, the obligation would extend just so far as the Australian provider's infrastructure and the gateway and not beyond that." Mrs Chidgey also noted with regard to the use of overseas services: "Clearly with international communication there is going to be part of service or infrastructure that is international. The obligation would only extend so far as they have the ability to control. If they choose to place some of their facilities in an offshore environment then this framework is designed to have a conversation about the risk of the particular arrangement they propose before it proceeds" (emphasis added).[1]

The PJCIS framed its recommendations to Government based on the testimony it received from AGD – particularly as it relates to this point. The most recent guidance contradicts the assurances that AGD gave to the Australian Parliament. It appears that the guidance attempts to 'shift the goal post' into a territory of protection that is nearly impossible or completely impossible to achieve. Consequently, we request the CIC amend its guidance to reflect the original intention of the law and as explained by the AGD during the hearing on 23 March 2017.

Over-the-top (OTT) services

Items 25 and 37 of the Frequently Asked Questions (FAQ) document address issues related to OTT services. We note that the headline of item 37 suggests that the item deals with CSPs providing or reselling OTT services. However, the actual explanation does not relate to CSPs but only to OTT providers that may meet the definition of a CSP. We recommend clarifying this item. It would also be helpful to either combine all OTT related items (also refer to item 25) or at least to keep all OTT related items closely together in the FAQ document.

Changes to core or sensitive systems or functions

Item 28 of the FAQ document contains the statement that "Any Change to core or sensitive systems or functions is likely to have a material adverse effect on the capacity of carriers and nominated carriages service providers to comply with their security obligation." This is an extraordinary statement which we reject given its absolute nature that does not appear to allow

[1] pp.3 and 4, Official Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Telecommunications and Other Legislation Amendment Bill 2016, Thursday, 23 March 2017

for further differentiation depending on the circumstances of the proposed change. We ask the CIC to elaborate on the basis for this statement.

Post-notification process

The CIC advised that in cases where the CAC found, upon notification of a change, that a change posed a risk of unauthorised interference or access that would be prejudicial to security, it would also provide an indication of how CSPs could potentially remediate such risk.

We note that CSPs require a formal notification from the CAC where CSPs have implemented measures that remediate the risks identified by the CAC, and where, as a result of such measures, the CAC has subsequently come to the conclusion that the proposed no longer constitutes a risk. We suggest that the CAC implement a process 'to close the loop' and provide adequate assurance to CSPs that their proposed change will not trigger a direction or other enforcement action.

We also recommend that the CIC provide some objective guidance on what kinds of mitigations might be acceptable in various scenarios.

Similarly, it would be helpful for both sides, if the CIC provided examples and guidance based on the learnings from notifications that have been received in the past and the remedial action that has been taken (and was deemed satisfactory). This would reduce the likelihood of multiple notifications for the same or similar changes.

Use of examples:

In the absence of a useful definition of 'material adverse effect', it is of even greater importance that the guidance material includes examples that would illustrate when a change would be deemed likely to have such material adverse effect.

Unfortunately, it appears from the discussions held at the recent stakeholder information session that all examples provided in the guidance material are still subject to the CSP finding that the change under consideration (and used as an example) is likely to cause a material adverse effect. This causes a circular logic as the examples ought to assist with determining what precisely constitutes a material adverse effect. We recommend presenting examples along with a statement along the lines of "In the examples presented below, it is likely that notification is required. However, CSPs may come to a different conclusion on the basis of their specific circumstances."

Drafting issues:

With regard to the use of the term 'material adverse effect', we note that the guidance material does not consistently include the 'likely' when referring to a material adverse effect, e.g. item 29 of the FAQ document only refers to "changes that do not have a material adverse effect". To allow CSPs to rely on the guidance material to the largest extend possible, we recommend consistently adopting a precise use of the term and an amended definition throughout all guidance documents.

We also recommend a consistent use of the terms 'should' (which suggests a degree of flexibility), 'must' and 'required' given the guidance is intended to provide clarification on a complex legal requirement.

We look forward to further engaging with the Critical Infrastructure Centre and other stakeholders on any TSS related matters.

Please contact Christiane Gillespie-Jones at c.gillespiejones@commsalliance.com.au if you have questions in relation to this submission.

Yours sincerely,

John Stanton
Chief Executive Office
Communications Alliance