Optus submission to the Parliamentary Joint Committee on Intelligence and Security:

Telecommunications and Other Legislation Amendment Bill 2016

3 February 2017

OPTUS

1. Introduction

1.1 Optus appreciates the opportunity to provide comment to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the proposed reforms in the Telecommunications and Other Legislation Amendment Bill 2016 ("the Bill").

1.2 In 2012, the PJCIS considered an earlier reference relating to these Telecommunications Sector Security Reforms ("TSSR"), and since then the Attorney-General's Department has consulted on several occasions with the telecommunications industry about the TSSR. Optus has responded to each of those consultations.

1.3 We acknowledge that the current Bill includes some adjustments made in response to views provided by stakeholders into each of those consultations, and we appreciate the efforts of the Government to respond to stakeholder concerns. Nonetheless, there remain some critical issues that Optus feels can be better addressed in the Bill, and it is on these issues which Optus will focus this submission. In particular:

- Notification requirements
- Consultation with industry
- Transparency and accountability measures of the Scheme

Optus is concerned with the threshold definition providers would have to work with when making a decision whether to notify the Attorney-General's Department. Optus considers that the functioning of the scheme would be enhanced if there is legislative underpinning for a new formal consultative mechanism, for the purpose of sharing information between Government, security agencies and industry participants on security risks and threat assessments. Optus also believes that it would be beneficial to the practical operation of the scheme if additional guidance is afforded in the Bill about the new regulatory role that will exist for the Attorney-General's Department (and the Communications Access Coordinator) and the framework in which it will operate.

1.4 Optus' concerns arise not from the proposed framework itself, but rather from the understanding that well-calibrated practical arrangements will be critical to the success of the TSSR. Should the appropriate checks and balances, design and measures to promote administrative practicality not be incorporated into the framework, it could serve to constrain the supply of services to the Australian market, limit the ability of Australian based suppliers to partner with global or regional providers, or impact investment confidence for telecommunications providers.

1.5 It is acknowledged in the Government's Cybersecurity Strategy, in the

Chapter on the desire for a national cyber partnership that:

"It is vital the public and private sectors work together to ensure individual and collective security, across the spectrum of cyber security challenges and opportunities that Australia faces."

While the measures proposed in the Bill have struck a reasonable balance, the changes proposed would further enhance the practical operation of the scheme and promote its chances of successful operation, consistent with the objectives of this related policy, which also recognises the benefits of transparency, accountability and information sharing partnerships.

1.6 Regional and global companies investing in Australia may wish to pursue specific business models that function successfully in other jurisdictions or consistent investment patterns or business processes across their operations. The compliance framework needs to be flexible enough to accommodate and be able to realistically adjust to the various commercial structures and ownership models that it may encounter.

1.7 The international nature of the communications industry supply chain, the global origin of threats and the Government's unique position to obtain intelligence not available to commercial players, mean that the success of such a scheme will require an open and transparent exchange of information between agencies, carriers and carriage service providers on risks and threat assessments.

1.8 As mentioned in Optus' submission to the PJCIS in 2012, Optus devotes substantial resources to protecting the security of its networks and the privacy of the communications that they carry. Optus also focusses on protecting the privacy of the customer information, including customer personal information that it collects and uses in the course of providing services to its customers and carrying on its business as a carriage service provider.

1.9 Optus has been co-operating with Law Enforcement and National Security Agencies since it was granted its initial fixed and mobile carrier licenses in 1992. Over that time there have been regular updates of interception legislation and carrier obligations, upgrades of capability within carriers, and improvements in practices of the law enforcement and national security agencies to take account of changing circumstances.

1.10 The TSSR framework must be designed to minimise 'inertia' in decision-making by arbiters of the scheme. Timely decisions and advice to the telecommunications industry are essential to promote certainty, particularly given the novel nature of the requirements and potential intrusion to current operations and business models.

1.11 Optus is a member of Communications Alliance, the Australian Mobile Telecommunications Association and the Australian Information Industry Association, and notes that these Associations, in conjunction with the Australian Industry Group, have jointly made a submission on this matter. This submission highlights the areas of Optus' prime concern, over and above the matters raised in the industry submission.

1.12 Optus remains committed to working with the Parliament to develop an appropriately robust framework for the Telecommunications Sector Security Reforms.

2. Notification requirements

2.1 There are a range of descriptions in the Bill, the Explanatory Memorandum and the Attorney-General's draft TSSR Guidelines intended to explain when a provider is required to notify the Communications Access Coordinator ("CAC") of any changes. These range from "early in the design phase of any planned changes" (page 25 of the draft Guidelines), "the stage at which a detailed business case is being prepared for the company Board for decision" (paragraph 128 of the EM), to where a provider "becomes aware that the implementation…of a change…proposed…is likely to have a material adverse effect on the capacity of the [provider] to comply with its obligations under subsection 313(1A) or (2A)" (section 314A(1) of the Bill).

2.2 These are all quite different stages of a provider's investment decision-making lifecycle and management processes, and in fact – despite their best intentions – a provider may not become aware of any adverse effects until the change has been implemented. Whilst Optus understands the need for flexibility in this requirement, there are some practical implications which will need to be addressed, as notification too early in the process may be unhelpful for the CAC to make a determination (for example, if the final technical configuration isn't fully understood because the name of the proposed vendor is not yet known), yet too late in the process (e.g. once a vendor has been chosen and a contract signed) will also be disruptive given the commercial impacts on the provider of an adverse assessment.

2.3 Sections 314A (1) and 314C (2) of the Bill require providers to make a judgement on likely "material and adverse effects" which in turn triggers a notification requirement. The net effect is to create a level of uncertainty for providers, as they are only able to make decisions based on their own understandings of any potential security issues and the risk

assessment of the security agency may be based on factors unknown to the provider.

2.4 The notification requirements are expressed in a way that creates a logic trap and an associated compliance risk for providers which is not satisfactory. The threshold for notification is whether a change is likely to have a material adverse effect on the providers' capacity to comply. However, if a provider forms its own view, based on the information it has available, that an event is not notifiable and it proceeds on this basis, it runs the risk that some 'after-the-event' investigation by the CAC draws a different conclusion and finds it in breach of the notification and security requirements of TSSR. This is the case, even though the security assessment may be based on information which the CAC or security agency had uniquely available to it and to which the provider was not privy when considering the threshold question. Regulated entities would have greater decision-making certainty if the drafting of the decision-making threshold for notification could be reviewed to accommodate this point.

3. Consultation with industry

3.1 One of the items that is not contemplated by the Bill is a formal consultative mechanism for information sharing between Government and industry. Given that the EM (in paragraph 10) advises that "The security framework will formalise the relationship between Australian Government agencies and C/CSPs to achieve more effective collaboration on the management of national security risks", Optus reiterates its previous recommendation that the Government consider implementing a formal, ongoing consultation process by which it can engage with industry for this purpose.

3.2 Such a consultation mechanism should be recognised formally within the legislation, and would be over and above the current bilateral discussions between Government and individual providers. A broader consultative process would encourage information sharing by industry and Government, and would assist in achieving the regulatory objectives of the TSSR "..to achieve national security outcomes on a cooperative basis" and "facilitate the early identification of potential national security risks" (paragraph 10 of the EM).

3.3 Paragraph 126 of the EM explains when providers must notify the CAC, i.e. "...of planned changes...which the C/NCSP has become aware are likely to have a material adverse effect on the capacity of the C/NCSP to

meet its security obligations..". To a provider, changing an existing vendor for a new one providing the exact same services, for example, may not be seen as "having a material adverse effect on the capacity...to meet...security obligations", however this is exactly the type of scenario that has been contemplated as needing to be notified to the CAC in case there is an adverse security assessment relating to the new vendor. Therefore, for providers to fully understand what types of issues they need to consider, ongoing consultation with Government with case studies and examples of what issues need to be considered are critical.

3.4 In fact, paragraph 132 of the EM advises that "C/CSPs would be expected to ...make themselves aware of guidance issued by AGD and information provided by security agencies, as appropriate, when assessing whether a proposed change is likely to have national security implications." An established consultative forum with industry would surely be the best way to manage this on an ongoing basis.

3.5 The early identification of potential threats and the ability to consider these in light of technological developments would also assist industry to better manage their capital and network planning processes, minimising the risk of retrospective applications of the TSSR for existing network components, which could be highly disruptive to the provision of communications services to Australian residents, businesses and government departments.

4. Transparency and accountability measures of the Scheme

REGULATOR FRAMEWORK

4.1 The proposed TSSR scheme further elevates the Attorney-General's Department (and certain roles within the Department, such as the CAC and the Attorney-General's Secretary) to a position of regulator of the communications sector, with a significantly expanded scope of responsibility and scale of operations. The Bill and associated documents do not currently discuss this change in role in any detail.

4.2 It would be helpful to understand whether the Government's regulator performance framework will apply to this expanded role and if so, whether information will be made publicly available about the KPIs applicable to fulfilling the functions of the expanded role as a regulator.

REGULATOR PERFORMANCE

4.3 Sections 314B(6) and 314D(6) of the Bill impose timeframes in which the CAC is required to respond to individual notifications and Security Capability Plans (SCP), however, they are silent on what occurs if these timeframes are not met by the CAC. This places an unacceptable level of commercial risk on providers.

4.4 The Bill should outline what the outcome will be if the CAC does not respond within the required timeframe. In Optus' view, if the CAC does not respond with a decision within the specified time limits, the notification or SCP should be deemed to be agreed unless formal notice is provided by the CAC of an extended assessment period with a revised notification date. Such a notice should be open to administrative review and further deadlines so it cannot be rolled over indefinitely.

REPORTING

4.5 A new requirement under section 315J has been added, requiring the Secretary of the Attorney-General's Department to submit annual reports to the Attorney-General on the operation of the provisions in the Bill. The Attorney-General will then be required to provide a copy of the report to Parliament.

4.6 Optus believes this measure has been introduced in an attempt to address stakeholder queries about the operation of the new regulatory function, and introduce a level of transparency in that regard. However, neither the Bill nor the EM provide any detail about what is required to be contained in those annual reports and what is the objective. Therefore, there is no certainty that the desired transparency and information about regulator performance will be supported by this reporting requirement and we recommend that section 315J in the Bill be expanded to detail what is expected to be contained in the report.

4.7 Such an approach is commonly seen in legislation, both in requirements placed on regulators to report on their activities and performance, and requirements for regulators to report on industry performance. Optus considers it is open for greater specificity to be provided in this instance.