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.

OPTUS

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Sent via email: pjcis@aph.gov.au

15 March 2017

Dear Secretary

OPTUS SUPPLEMENTARY SUBMISSION TO THE PJCIS INQUIRY INTO THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT BILL 2016

On Thursday 16th February 2017, Optus participated in the public hearing of the Parliamentary Joint Committee on Intelligence and Security (**Committee** or **PJCIS**) for the review of the *Telecommunications and Other Legislation Amendment Bill 2016.*

Following this, Optus has been asked to respond to two follow-up questions, which are responded to as follows:

Regulatory framework and performance

1. *Optus suggests the Bill should include additional information about the Attorney-General Department's role as regulator and whether the Government's Regulator Performance Framework would apply. In particular, whether the Key Performance Indicators would be made public (p6, para 4.1, 4.2):*

    a. *Is your key concern in raising this issue to ensure that the regulatory functions are accountable and transparent?*

    Yes. The practical effect of the Bill is to establish the Communications Access Coordinator (**CAC**) as a regulator with a substantially expanded set of obligations, a broader range of legislated decision-making duties to perform, and new powers under the Telecommunications Act which it has the discretion to exercise. These are in addition to its existing role under the Telecommunications (Interception and Access) Act. Because of this expanded mandate and the significance of the obligation being administered, in Optus' view it is appropriate in public policy terms for a formal framework to be put in place to provide accountability and transparency over the regulatory functions being performed by the CAC, the Attorney-General's Department and, in the instance of any directions being issued, the Attorney-General.

    b. *Which aspects of the Government's Regulator Performance Framework are most important to you? (I.e. a survey about industry satisfaction with the regulatory arrangements, public reporting of Key Performance Indicators etc.?)*

    Optus' submission referenced the Regulator Performance Framework as an example of one possible method to increase the transparency and accountability,

OPTUS

however Optus prefers that at least part of the performance requirements for the regulator be included in the legislation. There are plenty of precedents for this – for example, the *Australian Communications and Media Authority Act 2005*, which sets out a range of mandatory performance measures the ACMA must meet, including the details of what must be contained in the ACMA's annual reports to the Minister and to Parliament.

Whilst the current draft of the Bill mandates annual reporting, it is silent on the content of this report. From Optus' perspective, there should be a requirement for the CAC to report on a number of issues, including but not limited to:

- how many notifications it has received (individual and in annual plans);
- how many decisions were made;
- the timeliness of its decision-making process;
- feedback from stakeholders making notifications to the CAC;
- instances where direction powers were used;
- any learnings about the functioning of the Part of the Act it is administering;
- whether the information exchange between industry and Government is functioning;
- whether the proposed guidelines have been effective in assisting the implementation of the provisions;
- whether are any lessons for national security and critical infrastructure protection have been learnt;
- whether the notification and decision-making process has had any apparent impact on the level or rate of investment being undertaken by the communications sector;
- trends in threat and risk information and analysis relevant to this Part of the Act;
- the use of information gathering powers; and
- any breaches of security in the notification or decision-making process being administered by the CAC.

If the process administered by the CAC is not run efficiently and within the mandated timeframes, it has the potential to disrupt billions of dollars in investments made by communications companies each year, adversely impacting business plans and consumers nation-wide. Optus therefore feels it is prudent that the Bill is structured to provide greater specificity to the reporting available to Parliament on how the CAC has performed its regulatory functions. To the extent that it may be relevant to include issues sensitive to National Security in such reporting, there could be provision for special reporting on these aspects to the PJCIS or to the Inspector-General of Intelligence and Security.

Notifications requirement

2. *Optus suggests reviewing the decision-making threshold for notifications to take into account that industry may not be aware of specific threat and risk information (p4 and 5, para 2.3, 2.4):*

    a. *Could your concern be addressed by ensuring a regular flow of practical and timely threat advice from government to industry?*

OPTUS

Optus is concerned about two main aspects of the proposed information exchange between Government and regulated entities, namely that:

- there is a regular and timely flow of information between the parties; and
- the type of information is targeted for the specific purpose at hand and includes the type of threat information that is uniquely available to the Government, and is not currently available to telecommunications providers.

While regular, general briefings will be helpful they are unlikely to be of assistance to the major communications providers in meeting their obligations. Optus already receives 'traditional' IT threat security information (e.g. DDOS, hacking) from a range of sources. For example, Optus, together with Singtel, has formed strategic partnerships with a range of global security leaders like Trustwave, FireEye, Palo Alto Networks, Checkpoint and Akamai. Optus runs an advanced security operations centre in Australia, which is linked to Trustwave's global network of operations centres. This provides Optus and Optus' Business Division's corporate and government customers in Australia with access to comprehensive threat intelligence, threat data analytics and advanced security automation for incident response, backed by the elite SpiderLabs® team at Trustwave.

We note that the Bill requires Optus to:

(a) do its "best to protect" its infrastructure
(b) make decisions and judgements whether to notify a business development
(c) Engage in discussions or negotiations with the Communications Access Co-ordinator about possible risk mitigations

based on its own assessment of the potential threat to security as defined in the ASIO Act.

The CAC and its security advisors will make judgements on exactly the same set of issues buts its deliberations will be informed by the security apparatus of the Government and information it is able to obtain from its treaty partners. This is the information asymmetry which is of concern to Optus.

In the absence of targeted arrangements to even out this asymmetry, the regulated entities will be at a disadvantage in terms of calibrating their compliance responses and taking actions under the TSSR obligations compared to those that are judging the merits of their actions.

What is needed by regulated companies such as Optus is access to security and threat information which is specific to the requirements of the TSSR legislation. Often this information will be available uniquely through Government and security sources such as five eyes intelligence. For example, whether a specific piece of network equipment has a design flaw or a backdoor which allows unauthorised access, whether a particular vendor or applications maintenance support provider has flawed security record, whether certain unlegislated activities by agencies in foreign jurisdictions create and unacceptable risk for certain functions to be undertaken in that geographic location.

These are all examples of matters of which the very specific detail may be only available in classified form to Government, but which could be 'sanitised' and made

OPTUS

available to carriers in an unclassified form which could assist their judgements and decision-making under the TSSR.

It should also be noted that Optus has run an annual investment program in its networks and business operations of well over $1 billion for each of the last ten years. With investments of this magnitude, great weight is given to business certainty and early access to reliable decision-making information. In Optus' view, with the Government deciding to impose the additional duties and obligations on carriers in the form of the TSSR regime, it should share in the task of:

a) making the regime workable; and
b) ensuring that a workable mechanism is put in place to regularly share the information at its disposal, which is critical to the smooth functioning of the TSSR and which will help overcome the information asymmetry between the regulator and the regulated entity. This information should not be generic cyber threat information, it should be information tailored to the specific content of the TSSR.

Optus recommends the PJCIS provides specific guidance, either in the form of legislative amendments or statements of intent in related documents, that the Attorney-General's Department should establish regular briefings for industry which have the designated purpose of providing a forum for the exchange of information which has been tailored to be specifically relevant to the administration and decision-making required by both carriers and the Department under the TSSR scheme.

I trust that these responses assist the Committee in their determinations.

Yours sincerely,

Gary Smith
Head of Regulatory Compliance

Submission to the Parliamentary Joint Committee on Intelligence and Security on the *Telecommunications and Other Legislation Amendment Bill 2016*

(Telecommunications Sector Security Reform) February 2017

Joint submission by:
Australian Industry Group (Ai Group)
Australian Information Industry Association (AIIA)
Australian Mobile Telecommunications Association (AMTA)
Communications Alliance

3 Feburary 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY		**3**
1.	**INTRODUCTION**	**4**
2.	**IN-PRINCIPLE CONCERNS**	**5**
2.1	**MEETING THE OBJECTIVE – MINIMISING RISK AND PROTECTING AUSTRALIA'S CRITICAL INFRASTRUCTURE**	**5**
2.2	**EXAMPLES OF INTERNATIONAL COLLABORATIVE ARRANGEMENTS**	**7**
2.3	**INNOVATION VS LEGISLATION**	**9**
3.	**DEFICIENCIES OF THE LEGISLATION**	**11**
3.1	**LOGIC OF THE APPROACH**	**12**
3.2	**ASYMMETRY OF NOTIFICATION REQUIREMENTS**	**12**
3.3	**PROTECTION OF NETWORKS THAT ARE BEING 'USED'**	**13**
3.4	**DEFINITION OF SECURITY AND PROTECTION FROM 'ACTS OF FOREIGN INTERFERENCE'**	**13**
3.5	**NOTIFICATION OF CHANGES WITH LIKELY MATERIAL ADVERSE EFFECT**	**14**
3.6	**PREREQUISITE OF AN 'ADVERSE SECURITY ASSESSMENT'**	**15**
3.7	**MEANING OF 'ADVERSE SECURITY ASSESSMENT'**	**15**
3.8	**RESALE OF OVERSEAS SERVICES, OVER-THE-TOP (OTT) SERVICES**	**15**
3.9	**DISCRETIONARY AND VAGUE THRESHOLDS**	**16**
3.10	**RETROFITTING OF NETWORKS AND FACILITIES**	**18**
4.	**CONCLUSION**	**18**

EXECUTIVE SUMMARY

This submission is lodged by the **Australian Industry Group (Ai Group)**, the **Australian Information Industry Association (AIIA)**, the **Australian Mobile Telecommunications Association (AMTA)** and **Communications Alliance** (jointly, the Associations), which collectively represent the bulk of Australia's $100 billion ICT industry, including telecommunications Carriers, Carriage Service Providers (C/CSPs), vendors and intermediaries.

The Associations welcome the opportunity to comment on the *Telecommunications and Other Legislation Amendment Bill 2016* (also referred to as Telecommunications Sector Security Reform (TSSR)) and commend Government for its response – by way of amendments – to some of the concerns raised by Industry during 2015/16 in respect of the first and second exposure drafts of the *Telecommunications and Other Legislation Amendment Bill 2015*.

However, this submission outlines continuing areas of concern with the Bill as presented to the Parliamentary Joint Committee on Intelligence and Security, including that:

- the purpose of the reforms remains unclear;
- the onerous nature of the compliance requirements will act to hamper the responsiveness of C/CSPs to cyber threats;
- there is no established strategy to brief C/CSPs on the threat environment;
- there remain several significant areas of vague drafting in the Bill, including uncertainty as to the status of resale of overseas services; and
- the legislation itself does not exclude or at least limit the requirement for C/CSPs to retrofit or remove existing facilities, leaving open the risk that Industry could face very high costs to rebuild existing networks.

The submission points to more collaborative approaches to dealing with cyber threat to communications infrastructure that are being taken or contemplated in major international markets such as the USA, UK and Canada. The Associations strongly suggest that the benefits of adopting a more collaborative, less prescriptive and less onerous strategy be carefully considered and examined in Australia before enacting the TSSR legislation.

1. Introduction

The Australian Industry Group (Ai Group), the Australian Information Industry Association (AIIA), the Australian Mobile Telecommunications Association (AMTA) and Communications Alliance (the Associations), welcome the opportunity to provide input into the Inquiry by the Parliamentary Joint Committee on Intelligence and Security on the *Telecommunications and Other Legislation Amendment Bill 2016*, also referred to as Telecommunications Sector Security Reform (TSSR).

The four Associations collectively represent the bulk of Australia's $100 billion ICT industry.

The **Australian Industry Group (Ai Group)** is a peak industry association in Australia which along with its affiliates represents the interests of more than 60,000 businesses in an expanding range of sectors including: manufacturing, engineering, construction, automotive, food, transport, information technology, telecommunications, call centres, labour hire, printing, defence, mining equipment and supplies, airlines, and other industries.

The businesses which Ai Group represents employ more than one million people. Ai Group members operate small, medium and large businesses across a range of industries. Ai Group is closely affiliated with more than 50 other employer groups in Australia alone and directly manages a number of those organisations.

For more details about Ai Group visit http://www.aigroup.com.au.

The **Australian Information Industry Association (AIIA)** is the national body representing Australia's information and communications technology (ICT) industry. Since establishing 36 years ago, the AIIA has pursued activities aimed to stimulate and grow the ICT industry, to create a favourable business environment for its members and to contribute to the economic imperatives of the Australian nation. AIIA's goal is to create a world class information, communications and technology industry delivering productivity, innovation and leadership for Australia.

The Association represents over 400 member organisations nationally, including global brands, international companies, national companies, and a large number of ICT SMEs. Its national board comprises representatives from hardware, software, and services companies and represents the diversity of the industry.

For more details about AIIA visit https://www.aiia.com.au.

The **Australian Mobile Telecommunications Association (AMTA)** is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile carriage service providers, handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry.

For more details about AMTA visit http://www.amta.org.au.

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian

communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through Industry self-governance.

For more details about Communications Alliance visit http://www.commsalliance.com.au.

2. In-Principle Concerns

2.1 Meeting the objective – minimising risk and protecting Australia's critical infrastructure

A shared objective

Industry acknowledges that Australia's critical infrastructure, including telecommunications services and networks, remains at risk from espionage, sabotage and foreign interference. Industry strongly agrees that a level of collaboration amongst and between Industry, Government and other players in the critical infrastructure environment is necessary to protect against and minimise these risks. Industry clearly has a vested interest in ensuring that any relevant infrastructure is resilient to external attacks, including espionage, sabotage and foreign interference.

Accordingly, Industry players are commercially motivated to make very large investments in hardening and protecting their networks and communications infrastructure from attack. Industry has a proven track record of close and effective cooperation with Government agencies (and each other, within the confines of the law) to ensure a shared understanding of any potential threats and coordinated action at all levels.

Getting policy settings right

The Associations suggest that when calibrating the appropriate policy settings in this area, policy makers and Government should give considerable weight to the expertise of network providers in designing and safeguarding their networks and the clear commercial incentive that exists in a highly competitive sector to drive security by design in network architecture to ensure operational reliability and customer trust and loyalty.

While the Associations are pleased that the legislation reflects some of the feedback and proposed amendments that had been provided by Industry earlier in the process and discussed with Ministers' Offices, Departments and agencies, the overall approach of the legislation remains of concern.

For example, the revised legislation now includes the ability for a CSP to make use of a 'security capability plan', and this is an improvement.

However, Industry considers that the fundamental approach embodied in the legislation still falls short of meeting the overall objective of protecting critical infrastructure from the risk of espionage, sabotage and foreign interference in so far as the legislation is:

- onerous in terms of regulatory overhead and compliance risk;
- excessive in its focus on service and equipment introductory risks (assuming any associated risks are known by Government), neglecting emergent risks and any unknown initial risks; and
- establishes a set of obligations for Industry without placing an equivalent obligation on the Attorney General's Department to brief Industry on the threats against which Industry is supposed to protect its networks.

Shared responsibility

Industry submits that quick action and responsiveness are required to strengthen network security, minimise the incidence of attacks and approach threats proactively. Industry also notes that the TSSR regime appears to be founded on the incorrect assumption that security risks are known by C/CSPs before service introduction or equipment deployment occurs; whereas in practice, cyber threats may only emerge, or become known, after introduction/deployment. Industry's view is that the TSSR regime as set out in the legislation does not assist the responsiveness of C/CSPs and the wider ICT industry to emergent cyber threats. Worse, it may in fact divert scarce resources away from investing directly in addressing cyber security threats, to compliance overhead arising from the regime. It may reduce the ability for the ICT industry and its clients to proactively monitor and quickly respond to threats and breaches.

Further, there is no obligation established in the legislation for the Attorney-General's Department to work cooperatively and proactively with Industry in identifying, communicating and responding to threats and attacks (whereas such an obligation is established in Section 312 of the *Telecommunications Act 1997* (Act) for the Australian Communications and Media Authority (ACMA)). Government has asserted in Industry briefings that the value of the reforms will be through the delivery and sharing of additional cyber threat intelligence (which is currently unavailable to Industry and would remain unavailable without the reforms) but which, if known to Industry, could alter the way they manage and deploy safeguards in their networks. This assertion would seem to point to deficiencies in existing practices and speak to the necessity of a cooperative framework rather than additional regulation and the granting of additional powers to Government agencies. It cannot, presumably, be Government's intention to establish a regime of directions without evidence or corroboration of necessity.

Designing an effective and collaborative regulatory framework

The legislation, Explanatory Memorandum and the associated Guidelines[1] still fail to answer the fundamental question of what specific failings and/or weaknesses Government is seeking to address. Has Government already identified or become aware of specific failings and/or weaknesses in Industry's networks and not briefed Industry accordingly? It remains unclear how this additional layer of regulation and cost to Industry and intrusion into the commercial decision making processes of C/CSPs and carriage service intermediaries can be justified. The Explanatory Memorandum notes that the legislation is aimed at "introduce(ing) a regulatory framework to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications services and networks."[2]

The Associations strongly maintain that further adjustment of the reforms is needed to extend and maintain the security framework for the telecommunications industry in an effective and efficient manner.

The legislation instead introduces a regime that imposes requirements and obligations to create a one-way flow of information from C/CSPs to Government in relation to the design of networks and purchase of its components, rather than ensuring the supply by Government of detailed threat information that can be used by C/CSPs to protect against specific failings and/or weaknesses. The regime grants Government wide-ranging powers to intervene in a C/CSP's

- network design;

[1] Industry notes that no updated Administrative Guidelines have been provided along with the *Telecommunications and Other Legislation Amendment Bill 2016*.
[2] p. 2, para. 1, Explanatory Memorandum to the *Telecommunications and Other Legislation Amendment Bill 2016*

- vendor selection;
- procurement and M&A activities;
- service supply options, including resale of global or regionally based services; and
- use of global or regionally based network or business resources of multinational organisations.

In contrast, there is no corresponding obligation on Government to justify its actions, take responsibility for any unintended outcomes, bear the costs or deliver a practical and timely threat advice service. Nor is there any guidance or limitation on regulatory creep of the TSSR framework into services and networks that are non-critical.

Alternative arrangements as discussed in section 2.2 below are likely to produce better results while being less intrusive.

2.2 Examples of international collaborative arrangements

As outlined in the sections below, the TSSR regime runs the very serious risk that it will not be adaptable or flexible enough to tackle the risks that will emerge. Cyber threats are ever changing; risks and vulnerabilities will emerge as the concerns of the past are resolved. In this environment, traditional 'command-and-control' regulatory frameworks will not be agile enough to meet this 21st century challenge. It also runs the risk of unnecessarily increasing costs and investment risks of the telecommunications industry which will impact Australia's digital capability.

The Associations believe that it is crucial for the success of a robust and responsive national TSSR regime to be a collaborative, outcomes-focused framework. Indeed, Industry has a strong and well-established history of working cooperatively with the national security agencies to ensure that risks and threats are managed in a way that keeps Australia safe. We believe that more collaborative frameworks need to be developed than those set out by the legislation.

As in the previous submissions, the Associations note that in comparison to other relevant jurisdictions, the legislation is out of step and over-reaching. Consequently, we reiterate our concerns and point to preferred alternative and more collaborative approaches taken in the USA, UK and Canada.

USA

The **USA** takes a more collaborative approach to cyber security. In December 2014, the US Congress passed the *Cybersecurity Enhancement Act 2014*, a package of two key cyber security bills that will keep the National Institute of Standards and Technology (NIST) centred with the private sector on advancing voluntary, industry-led standards and best practices for cyber security. The combined bill will also support increased prioritisation of federal cyber security research, workforce development and public awareness – all areas that are critical to Industry's ongoing efforts to defend and protect against cyber threats.

In February 2015, the then President Obama also issued an Executive Order which calls for the Department of Homeland Security to develop a common set of voluntary standards for information sharing with organisations in the public and private sectors. Developing this baseline will enable all parties to quickly demonstrate their policies and security protocols and to develop best practice approaches.

At the end of 2015, before adjourning for the year, the US Congress passed the *Cybersecurity Act of 2015,* and the President signed the measure into law on December 18, 2015. The aim of this law is to defend against cyber attacks by creating a framework for the voluntary sharing of cyber threat information between private entities and the Federal Government, as well as within agencies of the Federal Government. The

legislation also contains provisions that aim to protect privacy by ensuring that personal information is not unnecessarily divulged. The goal of the legislation is to promote and encourage the private sector and the US Government to exchange cyber threat information rapidly and responsibly. The sharing of information is completely voluntary, but companies who share cyber threat indicators or defensive measures will receive legal liability safeguards if they comply with the appropriate privacy protections. There are also obligations upon Government regulators to develop policies and procedures as to what constitutes a cyber security threat and defensive measure as well as what constitutes personal information for the purposes of the regime, and how privacy and civil liberties will be protected.

In February 2016, then President Obama directed his Administration to implement the *Cybersecurity National Action Plan* (CNAP) which again focuses on a highly collaborative approach between Industry and Government agencies and is backed by significant Government investment.

UK

In December 2016, the **UK** Government launched the *National Cyber Security Strategy 2016-2021which* focuses on a collaborative approach to managing cyber risks to Critical National Infrastructure and sharing of information. Section 5.4.6. of the *National Cyber Security Strategy 2016-2021* expressly states

"The Government will:

- share threat information with industry that only the Government can obtain so they know what they must protect themselves against;
- produce advice and guidance on how to manage cyber risk and, working collaboratively with industry and academia, define what good cyber security looks like;
- stimulate the introduction of the high-end security needed to protect the CNI, such as training facilities, testing labs, security standards and consultancy services; and
- conduct exercises with CNI companies to assist them in managing their cyber risks and vulnerabilities."[3]

The UK Government has also implemented an independent validation for vendor product security claims, known as CESG Claims Tested Mark (CCTM) and Certified Product Assurance (CPA). In addition, one particular case has concluded an agreement with one vendor whereby their company absorbs the cost of extensive evaluation of carrier grade network equipment to be deployed in the UK. Hence, this vendor has established an evaluation centre for this purpose. To date, we are unaware of any evidence of suspicious implants or code in the equipment they have examined per their 2015 Annual Report.

Australian context

While this approach is not fool-proof, it is worthy of consideration as part of a broader solution, which allows the Attorney General's Department to evaluate equipment independent of the Australian telecommunications sector (and largely the vendor) at no cost to them. In addition, the Government could use the Cyber Security Growth Centre to lead this initiative and develop a collaborative environment where Industry and Government can work together in securing the critical infrastructure programs.

[3] p.41, National Cyber Security Strategy 2016-2021, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Canada

The Associations also suggest exploring the approach that the **Canadian** Government appears to be contemplating. The Associations understand that Canadian Industry has been asked to develop a cyber security framework that may impose legislation or regulation if no feasible framework can be agreed with Industry. The recent public consultation on Canada's future cyber security strategy (concluded in October 2016) again stressed a collaborative approach between all stakeholders including providers of communications infrastructure. Rather than taking a prescriptive regulatory approach, the Canadian *Action Plan for Critical Infrastructure*[4] sets out a number of collaborative actions and educational measures across Government, Industry and infrastructure owners to combat cyber threats.

A preferred approach

Against this background, the Associations reiterate that a preferred approach would be to reconsider the roles and responsibilities of risk assessment through collaborative sharing of information about actual and potential threats, and what tools and techniques are recommended to ensure appropriate action is taken to protect all the components that make up networks (i.e. hardware and software). It should also consider impacts on ordinary business activities and innovation. Industry suggests that suitable fora could be established that encourage sharing of information by industry (jointly and on an individual C/CSP level) and Government disclosure of such information as required for C/CSPs to protect their networks. Such an approach will enable the participants to develop arrangements for sharing experiences and expertise between the various stakeholders as well as guidelines for sharing information with the community with the aim of strengthening ICT threat protections more generally.

Industry-developed frameworks are likely to be significantly more flexible with regards to the frequent adaptations required to keep up with technological progress and market changes.

It is imperative for Australia to leverage the important activities undertaken in the USA and elsewhere and to adopt, as much as possible, globally-consistent approaches. This will enable Australian agencies to work more effectively in concert with key foreign jurisdictions, and ensure technology that is developed to address threats is consistent across the globe. Importantly, Industry urges Government to establish effective cooperation mechanisms between Australian and overseas agencies to obtain improved and timely threat information and cooperation and assistance to more effectively fight cyber crime.

Also, by leveraging standards and best practices from other jurisdictions, Australia can utilise the techniques and tools that are available at economies of scale, rather than developing standards and practices that are out of step with global best practice and therefore considerably more expensive.

2.3 Innovation vs legislation

Against the background of the aforementioned detrimental consequences for innovation, the Associations point out that the TSSR regime appears to be at odds with the *National Innovation & Science Agenda (NISA)* which sets out a whole range of measures intended to foster innovation. The NISA specifically addresses the lack of collaboration which, as Industry believes, is not only confined to collaboration (or lack thereof) between academia and Industry but equally applies to collaboration between Industry and Government institutions in the area of cyber security. Importantly, the stated

[4] Refer to https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/index-eng.aspx

aims of the Australian Cyber Security Growth Network (ACSGN) established in December 2016 (commencing operations in early 2017) are to:

- "bring together industry, researchers and governments to create a national cyber security innovation network
- develop a national strategy for Australia's cyber security industry to become a global leader and attract investment from multinationals
- coordinate cyber security research and innovation to reduce overlap and maximise impact."[5]

The TSSR legislation is at odds with these stated aims as it would mean the implementation of a heavy-handed and costly regulatory regime which is likely to impede innovation without necessarily achieving the desired aim.

Australia will reap an 'innovation dividend' if regulatory structures, including the development of standards, operate on a collaborative basis rather than placing undue requirements on Industry. Industry is best placed to innovate and develop technical solutions that respond in a timely and effective way to cyber threats. Placing excessive regulatory requirements on Industry slows down responsiveness and will be more likely to stifle innovation necessary to keep pace with the increasing sophistication of cyber threats. Businesses will focus on minimising exposure to regulatory imposts or on compliance instead.

The Associations reiterate the potentially negative consequences of the reforms on businesses and innovation, particularly in the context of the Internet of Things (IoT).

Impact on Software-Defined Networks and Network Function Virtualisation

Unintended (or willingly accepted) impediments to ordinary business activities and innovation are a significant and very real threat, including in the area of Software-Defined Networks and Network Function Virtualisation (SDN/NFV). These technologies are at the forefront of next-generation network developments, carry functionality that is central to the development of 5G mobile networks and the game-changing IoT and afford important innovation opportunities to Australia.

The shifting of a cutting-edge SDN testbed project (called REANNZ) out of New Zealand to Australia and the USA, which (so far) have less intrusive legislation, in early 2015 is just one example of the unintended impact of legislation containing notification requirements similar to those in the Australian TSSR legislation. The companies involved in the project stated that the shift offshore was a direct consequence of the notification requirements for network changes (which often occur on a per-second basis in an SDN environment) and the associated compliance work, legal uncertainty and exposure associated with the New Zealand *Telecommunications (Interception Capability and Security) Act 2013*. (See also http://www.zdnet.com/article/surveillance-law-prompts-shift-for-google-sponsored-sdn-test-bed.)

As is the case in NZ, it is likely that Australian authorities will take time to get up to speed on very new technologies and their use within networks and this can delay or deny implementation of such technologies as authorities adopt a conservative approach and 'err on the side of caution'.

Furthermore, experience from NZ shows that authorities seem to have the expectation that all new capabilities go through months of testing and evaluation prior to deployment. This is not the case for many smaller C/CSPs (and also larger C/CSPs) where a fast time-to-market and the ability to quickly respond to customer demands are crucial for commercial success.

[5] Refer to http://www.innovation.gov.au/page/cyber-security-growth-centre

As the report *NFV Hardware, Software, and Services* by IHS Infonetics indicates "one of the biggest drivers for NFV is the ability to scale services up and down quickly and introduce new network services more efficiently and in a timely manner." The report also notes that "All major operators are either now deploying NFV or plan to within the next few years. Telcos generally believe that NFV and its SDN (…) companion are a fundamental change in the telecom network architecture that will deliver benefits in service agility and new revenue, operational efficiencies and capex savings."[6]

Equally, simply launching a new service in the market could trigger a C/CSP's notification requirement thereby introducing delay and a significant degree of uncertainty which may render a project or service unviable in the fast-paced ICT environment. In fact, from a practical perspective, under the proposed TSSR regime, C/CSPs would potentially have to notify the initial NFV infrastructure, SDN elements and orchestration arrangements as well as major initiatives to move new or additional elements from a legacy to an SDN/NFV environment. This potentially implies a TSSR requirement for multiple notifications to the Communications Access Co-ordinator (CAC) resulting from expanded uses of the same underlying infrastructure.

This means that the increasing adoption in Australian networks of SDN/NFV technology will likely place time and resource pressure on the administration of the TSSR by the CAC, and mean that the 'regulatory risk' of projects and initiatives being delayed by CAC decision-making times is more prevalent. In practice, the likely major implications of SDN/NFV for the TSSR in its current form are to significantly add to the work-load of the CAC (number and frequency of decisions), of the national security agencies (number and frequency of risk assessments), and to increase the administrative burden on C/CSPs (notification requirements, and potential for delayed regulatory decision-making).

Industry notes that the security capability plans, that the revised draft legislation has introduced, while being very useful in many areas, will not be able to overcome the problems that the reforms pose for flexible and fast innovation processes.

Given the above, the implementation of the TSSR regime carries the real risk that investment in new network innovation in Australia will be halted or driven offshore. Australia will be at risk of being left behind in the adoption of game-changing technologies.

In light of the intended focus on innovation, collaboration and the ACSGN, it appears even more evident that the proposed reforms do not strike an appropriate balance between risk and opportunity.

Equally, and as set out in previous submissions, the Associations note the lack of an overarching cyber security framework developed prior to the implementation of components such as the data retention regime or the TSSR. The absence of this overarching framework is not only likely to result in overall inefficiencies and potentially sub-optimal policies and regulations, but also practical difficulties.

3. Deficiencies of the Legislation

The Associations commend Government for the revision of the second Exposure Draft to attempt to address a number of issues raised by Industry during the consultation process.

[6] Quotes taken from CommsWire Daily, 20 July 2015, *NFV MARKET TO GROW 500% IN FOUR YEARS*

However, apart from the previously mentioned concerns with the general premise of the legislation, the legislation as tabled gives rise to some new concerns and still carries some (previously highlighted) drafting concerns.

3.1 Logic of the approach

The basic logic of the approach of C/CSPs having to notify the Attorney-General continues to be fundamentally flawed: if, in accordance with the revised Section 311 and 313 of the Act, C/CSPs have a "duty to do their best to protect telecommunications networks and facilities from unauthorised interference, or unauthorised access", then anything "likely to have a material adverse effect on their capacity to comply with this duty" cannot exist – irrespective of any notification and potential subsequent authorisation – without already causing a breach of the obligation "to do their best to protect". Doing something that may adversely affect protection while not breaching the obligation cannot co-exist with the duty to do one's best to protect, whether notified or authorised, or not.

If additional requirements in relation to the current Section 311 and 313 of the Act are deemed necessary at all, the principle ought to be that C/CSPs have a duty to do their best to protect their networks, and in case they seek to do one or more of the following: [list of specific items], notification is required.

3.2 Asymmetry of notification requirements

The notification requirement in section 314(A) of the Act provides a trigger for C/CSPs to engage with Government early in their planning, design and procurement activities. However, there is no equivalent obligation on Government to proactively notify C/CSPs early when it becomes aware of security threats to C/CSPs' telecommunications networks or facilities.

The TSSR regime leaves it up to C/CSPs to determine the potential future threats and vulnerabilities and to make an assessment on whether or not a proposed change to their networks or facilities may adversely impact on their ability to meet their security obligations. The TSSR then requires C/CSPs to implement the appropriate measures to manage these risks.

It appears highly inefficient that C/CSPs are obliged to proactively notify Government of proposed changes to their networks (i.e., outsourcing, offshoring, equipment procurement or change in management) and proposed risk mitigation strategies while Government is not compelled to equally notify C/CSPs of any potential or real security threats to networks and facilities. This means that C/CSPs may receive an adverse security assessment and, consequently, commit scarce resources to developing risk mitigation strategies based on incomplete or no threat information from Government. This is an inefficient process and is likely to add to compliance costs which ultimately will be borne by consumers.

Proactive and early threat warnings from Government will not only assist C/CSPs in developing risk mitigation strategies but may also assist in including specific items in their annual budget cycle to implement the appropriate measures to manage potential vulnerabilities identified by Government. This will assist in reducing the already high regulatory cost burden on C/CSPs.

The Associations believe that Federal Government must be compelled to proactively make C/CSPs aware of any known security threats to their networks and facilities. This could be done through the establishment of a Federal Government 'single point of truth and advice facility', such as a Threat Advisory Service.

3.3 Protection of networks that are being 'used'

The Associations welcome the limitation on the requirement "to maintain competent supervision of, and effective control over, telecommunications networks and facilities" (new Section 313(1B)) to networks that C/CSPs own or operate. We also appreciate the amendment of the legislation to no longer include a requirement on intermediaries to exercise such supervision and control (previously new Section 313(2B)).

However, we note with concern that, in accordance with the new Section 313(1A) and 313(2A), C/CSPs as well as intermediaries now have an obligation to do their "best to protect telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access" [emphasis added]. It is unclear what 'use' may actually entail and, maybe more importantly, what would be required of C/CSPs/intermediaries to protect networks that they are merely using. Does the law envisage additional contractually agreed liability obligations between C/CSPs/intermediaries (which would already be problematic) or is something else/more required of C/CSPs/intermediaries to fulfil this obligation?

By way of example, what would be required of CSP A, on whose network a call is being originated (i.e. one of its customers makes a phone call) and this call is being terminated on CSP B's network? Obviously, CSP A is 'using' CSP B's network but has no means to protect that network from interference or access.

3.4 Definition of security and protection from 'acts of foreign interference'

The Associations continue to be concerned about the consequences resulting from the introduction of the definition of security as "the protection of, and of the people of, the Commonwealth and the several States and Territories from: (i) espionage, (ii) sabotage, […] (iv) acts of foreign interference" (*Australian Security Intelligence Organisation Act 1979*). Comments on this issue provided in previous submissions on the TSSR, in our view, remain equally valid and, consequently, ought to be re-stated.

It is a common feature of today's business practices by C/CSPs to take advantage of the utility and cost effectiveness of infrastructure located outside Australia.

It is unclear how C/CSPs captured under the legislation would be able to comply with their duty to do their best to protect their infrastructure from espionage, sabotage and acts of foreign interference while simultaneously still fulfilling relevant obligations that offshore legislation may impose onto them.

It is conceivable or even likely that C/CSPs that are making use of network facilities or other infrastructure located offshore may be required to comply with requests by foreign Governments and/or security agencies which could be construed by Australian agencies to amount to 'espionage' or 'interference' but which are lawful under the terms of relevant legislation in that jurisdiction.

This concern is compounded by the inclusion of the requirement to "maintain competent supervision of, and effective control over, telecommunications networks and facilities" into the legislation (noting that this only applies to infrastructure owned or operated by the C/CSP) as this requirement pertains to Australians and Australian networks, including those offshore.

The conclusion therefore is that TSSR will have the serious consequences of:

- preventing the use of network facilities or other infrastructure located offshore and the supply of associated services; and/or

- creation of smaller scale, higher cost and delayed services using onshore infrastructure; and/or
- customer migration to direct supply from offshore entities (noting for example that this is common already for social media services, and these entities already offer communication services, including text, voice and video).

The requirement, arising from the definition of security in the *Australian Security Intelligence Organisation Act 1979*, to protect telecommunications networks and facilities from 'acts of foreign interference' remains problematic as it is unclear what measures might be regarded as sufficient protections from such interference. For example, would additional security and access controls and/or an ability to log, within Australia, any lawful access made to Australian systems offshore be sufficient to fulfil the requirement of protection against 'acts of foreign interference'?

The Associations seek a clear description of measures that are deemed acceptable to demonstrate such protection, either in the legislation itself (preference) or at least in the Explanatory Memorandum.

3.5 Notification of changes with likely material adverse effect

In addition to the comments provided in section 3.1 of this submission, we note the following:

The Explanatory Memorandum correctly notes that the new Section 314A of the Act is modelled on the existing Section 202B of the *Telecommunications (Interception and Access) Act 1979* (which will be amended to exclude application to the new Section 313(1A) and 313(2A) of the Act).

However, it is very important to note that the fact that the new Section 314A is being modelled on an existing obligation must not be understood as constituting appropriate regulation for the telecommunications industry. This is the case as the TSSR legislation as currently drafted extends the application of Section 313 to include the obligation to do the "best to protect telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access" [emphasis added]. The significant extension of the application of Section 313 and the lack of clarity as to what the 'use' of a network may entail and which consequences such 'use' brings with it (as discussed in section 3.3 above) mean that a mirroring of Section 202B of the *Telecommunications (Interception and Access) Act 1979* is not appropriate and cannot serve as an argument that Industry ought to be used to the requirements stipulated in Section 202B of *Telecommunications (Interception and Access) Act 1979*.

The Associations contend that the notification requirements as drafted in the new Section 314A fail to provide a useful mechanism due to the very wide scope of 'changes' that, subject to the test of material adversity, are notifiable. As currently drafted, the (non-exhaustive) list of 'changes' implies that just about anything that a C/CSP might do in the normal course of network and system management might be deemed a notifiable change. This is extremely problematic as the notifiable changes and the material adversity test now relate to the definition of security in accordance with the *Australian Security Intelligence Organisation* Act 1979 which brings with it its own issues as discussed in section 3.4 above.

The issues around an overly wide and ill-defined scope of 'changes' are exacerbated by the fact that 'notifiable equipment' (Section 314A(2)(b)) includes all carriage related equipment, thereby – in addition to the wide scope of the term itself – creating an incredibly wide application of 'changes'.

It also appears impracticable to include the procurement of any equipment that is located outside Australia (Section 314A(20)(c)) into the list of potentially notifiable changes. It is fair to say that almost all network components for C/CSPs are manufactured overseas and, hence, would fall under this category of changes. It not clear which criteria C/CSPs would be required to apply to assess whether or not the procurement of equipment overseas would be likely to result in a materially adverse effect.

We are aware that the Explanatory Memorandum notes that C/CSPs are free to go ahead with any notified changes irrespective of a response from the CAC. This is only a theoretical option and not practicable – given the large costs and contractual obligations involved in many network changes it is highly unlikely that a C/CSP would choose to implement changes without having the 'go' from the CAC.

Against this background, it is concerning that the CAC will be forming a view on the material adversity of changes without a formal security assessment and/or formal criteria. Additional guidance prior to the passage of the legislation would be required to address those concerns. In this context, also refer to our comments in the next section.

3.6 Prerequisite of an 'adverse security assessment'

It is concerning that the requirement of an adverse security assessment only applies to the directions powers of the Attorney-General but not to the notification and consultation processes that precede the direction. This allows the Attorney-General to apply pressure onto C/CSPs without a formal basis for doing so. The Associations request that the adverse security assessment be a prerequisite for the entire process rather than just its last step.

3.7 Meaning of 'adverse security assessment'

We also note with concern that an adverse security assessment may only be an 'opinion', 'advice' or 'recommendation' within the meaning of the *Australian Security Intelligence Organisation Act 1979*. Given the potential consequences associated with such an assessment, the Associations believe that an assessment must be based on evidence and a formal assessment of risk.

It also appears that there is a possibility that the real reasons for an adverse assessment may be withheld from the C/CSPs and even the Administrative Appeals Tribunal on appeal. The Associations request that the legislation provide a secrecy framework that allows the grounds of any adverse assessment to be properly reviewed in camera. It is not acceptable that the whole process can be based on an 'opinion' which may be formed on no or little evidence and cannot be effectively appealed.

3.8 Resale of overseas services, over-the-top (OTT) services

Importantly, the legislation continues to only apply to a subset of the Australian telecommunications sector, i.e. C/CSPs and carriage service intermediaries, but it does not apply to overseas OTT services. The legislation fails to adequately recognise the evolution that is occurring in the supply of services over the internet. The regulatory burden of the reform falls onto a subset of the global market place for the supply of services, i.e. the burden only falls on Australian-based C/CSPs, including intermediaries as defined in the Act. Overseas service suppliers providing OTT services will not be subject to the TSSR. An Australian based C/CSP simply reselling OTT services faces substantial regulatory uncertainty and regulatory risk under the TSSR framework.

Industry contends that a C/CSP should only be required to take action under the legislation if the supply by the Australian C/CSP adds substantive security risk. The obligations of C/CSPs should be assessed solely on the basis of the application of the following iterative analysis:

- the level of security risk that applies if the service is obtained directly from the service supplier;
- the level of security risk that applies if the service is obtained via the C/CSP; and
- the steps that can be implemented by the C/CSP to address any added security risk.

As an example, consider the supply of a webmail service by the fictitious international service provider CanndyTel. Any Australian can subscribe to CanndyTel and obtain an email address of the form user@CanndyTel.com. Any security risk inherent in CanndyTel services will be unregulated by the TSSR framework. The user may also obtain other services such as cloud storage, word processing, spreadsheet and database capabilities from CanndyTel.

An Australian C/CSP may purchase services from CanndyTel but use their own brand name for sales purposes. For example, the fictitious Australian C/CSP Volptra may obtain email addresses for its customers in the form user@volptra.com.au, noting that the service is still supplied entirely by CanndyTel. Any security risk inherent in the CanndyTel service will remain unchanged by Volptra.

However, under the TSSR, the Australian C/CSP Volptra now appears to have an obligation to do its best to protect facilities (note our additional comments on 'facilities' in section 3.9) which it 'uses' to provide the service. This obligation places the Australian C/CSP Volptra at a competitive disadvantage compared with overseas providers offering the same service.

(Note that while the service provider names are fictitious, the service supply scenarios are based on real cases that have been blocked, or attempted to be blocked, by the Attorney-General's Department staff in the past.)

The Associations are very concerned that, as a result of the reforms, Australian-based C/CSPs will be relegated to play minor, low-value roles in the supply of internet services and that internationally-based companies will dominate the supply of value-adding OTT services, resulting in a negative effect on competition, the industry and the overall framework required to assist in achieving the TSSR policy objective.

The reforms thus establish a lose-lose-lose outcome for Australia:

- customers lose the opportunity to deal with locally-based C/CSPs;
- Australian C/CSPs face a competitive disadvantage in the supply of value-added services and thus the revenue to fund further investments in Australia; and
- any security benefits that the reforms claim to provide do not materialise as the offshore providers, who will continue to provide their services to Australians, are not regulated by the reforms.

3.9 Discretionary and vague thresholds

It remains the case that the obligation to protect networks and facilities from unauthorised interference and unauthorised access and to maintain competent supervision and effective control is vague and open to discretionary interpretation in the absence of a clear definition of these terms, particularly with regards to the term 'facilities'. We request that further explanation of these terms be included in the Guidelines.

Section 7 of the Act defines facility as "any (...) equipment, apparatus (…) or thing used, or for use, in or in connection with a telecommunications network." Consequently, it is conceivable that the term 'facility' could be interpreted to encompass cloud computing and cloud storage solutions implemented by C/CSPs as any supporting equipment would appear to meet the above definition. This has the potential to significantly broaden the regulatory burden that C/CSPs face under the regime and will leave them at a competitive disadvantage compared with suppliers of equivalent services that are not C/CSPs.

Experience with other current security-related legislation has shown that the ex-post interpretation of undefined (and even defined) terms in the technical areas of communications create confusion at best and randomness at worst, and ought to be avoided.

Importantly, Section 315B of the Act contains very broad powers allowing the Attorney-General to give a C/CSP a direction "to do, or to refrain from doing, a specified act or thing within the period specified in the direction" if the Attorney-General "is satisfied that there is a risk of unauthorised interference with, or unauthorised access to, telecommunications networks or facilities that would be prejudicial to security."

While the legislation includes the requirement that such a direction by the Attorney-General can only be given after an adverse security assessment in respect of the C/CSP has been obtained by the Attorney-General, the direction powers rest on terms and concepts that lack definition within the legislation and/or transparency.

Neither the level nor nature of risk or prejudice to security has been defined. It appears that any kind of risk would suffice as long as an adverse security assessment has been given. This is particularly problematic as the criteria for arriving at an adverse security assessment are not known to Industry and appear not to be subject to a balance of probabilities test.

This issue is again compounded by the provision that in making his decision to issue a direction, the Attorney–General must have regard to a number of matters, including costs to the respective C/CSP and consequences for competition, but give the greatest weight to the adverse security assessment.

This is particularly concerning as current Industry experience shows that a decision for an adverse security assessment by Government agencies is often lacking transparency and rationale. It is very worrying that the legislation does not provide for increased transparency or forensic evidence for an adverse security assessment. Mere assertions that the threshold for an adverse security assessment is very high do little to create sufficient certainty for large financial investments.

Industry urges Government to make the relevant criteria for such an adverse finding available to Industry to allow for greater transparency and scrutiny.

Industry also requests that the risk of unauthorised interference and access be specified as substantial and imminent to ensure that these far-reaching powers will only be exercised where absolutely required.

The Associations also note that the meaning of 'prejudicial to security' ought to be defined within the legislation itself instead of being described within the Explanatory Memorandum[7].

[7] p. 14, para. 63, Explanatory Memorandum to the *Telecommunications and Other Legislation Amendment Bill 2016*

3.10 Retrofitting of networks and facilities

Section 313(1) places security obligations on C/CSPs without further distinction of the age of the systems, networks and facilities (jointly systems) or whether systems are already existing and in place vs. newly installed systems.

Given the very high bar placed by the definition of security, the large financial commitment that telecommunications infrastructure typically represents and the risk that a retrofit direction could cost a C/CSP hundreds of millions of dollars – or more – a simple assurance in the Explanatory Memorandum and Guidelines that non-compliant systems will not be penalised does not create sufficient certainty for C/CSPs.

At the very least, the legislation itself ought to be amended to reflect the intention to not require retrofits except in rare and extremely serious circumstances.

Further, the legislation should include a sunset clause on the ability to issue a direction for a network retrofit. The legislation could, for example, state that Government's right to require a retrofit expires 12 months after the expiry of the implementation period (i.e. two years after the date of Royal Assent). This would provide at least some element of certainty for C/CSPs as to the longevity of existing systems.

4. Conclusion

The Associations look forward to continued engagement with Government, the Parliamentary Committee and relevant agencies on the mutual objective to ensure the robustness of national communications infrastructure and to devise appropriate tools to further that aim.

However, as outlined in this submission, the Associations do not believe that a comprehensive case for TSSR has been made. In its current form, the legislation is too discretionary and vague and is lacking two-way cooperation and information, thereby imposing substantial costs, uncertainty and regulatory risk onto the entities proposed to be regulated. The legislation is an over-reach and an unnecessary imposition of inflexible black-letter law when a more flexible, proactive, informative and collaborative approach (as is being implemented in other jurisdictions) would be more effective in protecting Australia's telecommunications infrastructure.

Telecommunications and Other Legislation Amendment Bill 2016

Questions on Notice for Industry Associations

Subsequent to Public Hearing on 16 February 2017

Question on Notice agreed at hearing:

1. Industry associations note that the Bill applies only to a subset of the Australian telecommunications sector (i.e. it applies to C/CSPs and intermediaries, but not to over-the-top service providers). Industry suggests the Bill 'fails to adequately recognise the evolution that is occurring in the supply of services over the internet', and that an Australian based C/CSP 'simply re-selling over-the-top services' will face substantial regulatory uncertainty and regulatory risk under the framework. Industry further suggests that a C/CSP should only need to take action under the proposed legislation if the supply by the Australian C/CSP adds a substantial security risk (p15, para 3.8).

    - As discussed at the public hearing, please develop a proposal outlining any additional amendments you seek to the Bill, Explanatory Memorandum and/or Administrative Guidelines?

INDUSTRY RESPONSE:

As per our submission, Industry believes that a C/CSP should only be required to take action under the legislation if the supply of the over-the-top (OTT, e.g. Skype, WhatsApp, Facetime) service by the Australian C/CSP adds substantive security risk. The obligations of C/CSPs should be assessed solely on the basis of the application of the following iterative analysis:

- the level of security risk that applies if the service is obtained directly from the service supplier;
- the level of security risk that applies if the service is obtained via the C/CSP; and
- the steps that can be implemented by the C/CSP to address any <u>added</u> security risk.

This approach could be incorporated into the legislation in two ways:

- By amending s314A(1), e.g. by adding. "…and, where the change relates to the resale of an OTT service from a non-Australian provider through an Australian carrier or carriage service provider, the resale of that service through the Australian carrier or carriage service provider substantially increases the likelihood or potential severity of a materially adverse effect (on the ability of the carrier or carriage service provider to comply with its obligations under subsection 313(1A) or (2A)) already inherent in the OTT service as provided and available to the Australian public from the non-Australian provider."; or
- By adding a 'class exemption' (creating a new s314A(4)) to the law, e.g. "Section 314 does not apply to changes…[and then something along the lines of the above]."

Note that the above would require the insertion of a definition of OTT services in s7 of the Act.

Security Obligation

2. Industry associations are concerned that C/CSPs and intermediaries will be subject to an obligation to protect networks and facilities owned, operated and <u>used by</u> the C/CSP from unauthorised access and interference. Industry has indicated concern

about what the term 'use' may entail and what would be required of C/CSPs and intermediaries to protect networks they are 'merely using'. Industry has sought clarification about the sorts of measures that could be put in place to demonstrate compliance with this obligation (p13, para 3.3):

- Can you please explain your concerns about the term 'used by' and why you consider it to be difficult to demonstrate compliance against this aspect of the security obligation (section 313)?

INDUSTRY RESPONSE:

It should be noted that a CSP has the relationship with an end customer while carriers own and operate the network infrastructure required to enable a communication to be carried. A CSP may also be a carrier, however, in many cases they may neither own nor operate network infrastructure to support the delivery of a communication, as that is the role of carriers.

CSPs can have many arrangements to deliver communications for their customers. These may be via a network that they own or operate under an Australian carrier licence, or they may contract with one or more carriers who may be Australian or non-Australian entities.

Where a CSP is also a carrier, they may also use carrier infrastructure owned and operated by another carrier to deliver a communication within Australia (e.g. national roaming) and they may, or may not, own infrastructure for any international component of a communication. Carriers may own and operate infrastructure within Australia, or they may use local bearers to deliver communications to a non-Australian location where routing is managed.

The obligation of s313 goes to the protection of networks and facilities (refer to the Industry Response at question 4 regarding a discussion on the term facilities) that they own, operate or use. C/CSPs accept an obligation to do their best to protect networks that they own or operate and, consequently, the obligation to maintain competent supervision of and effective control over those networks makes sense. However, it is impossible for C/CSPs to directly protect networks that they use but do not own or operate (say under a wholesale arrangement with another carrier), precisely because they cannot exercise competent supervision of and effective control over those networks. Where the networks they use are located in Australia, network operators already have obligations of their own under TSSR, so it is not necessary to extend the obligation to wholesale customers of network operators who have no control over the infrastructure.

The transmission of all forms of communications in a very large number of cases implies the use of networks that providers have no direct control over, do not own, manage or operate.

Note that on its way to its destination, voice and data communications will make use of 'least-cost routing' arrangements that are used globally – for example, the voice bearer traffic of a call may be passing through a number of Australian and/or non-Australian networks. The voice signalling traffic required to connect and disconnect the call may yet again use other Australian and/or non-Australian network parts. In addition, the call routing, i.e. which networks are being used, may be dynamic and/or automated and change from hour to hour or even more frequently. Once a call leaves a network used by a CSP or a

network that a CSP operates, that CSP is unable to protect the networks that are being used in the course of this communication.

Consider the following examples:

1. A communication is originated in Australia by a customer of CSP A on an Australian network used by CSP A (who may, or may not, own or operate that network) and routing is carried out dynamically in one or many non-Australian locations and then routed back into Australia on one or more other Australian networks, that may, or may not be, owned or operated by CSP A.
   In this example, other Australian entities may have the obligation to protect their network assets within Australia, effectively meeting the aims of the legislation. The non-Australian portion cannot be 'protected' by CSP A as they may have no control of those networks and may have no control of the routing used by the carriers bearing that communication to its destination.

2. A communication is originated in Australia by a customer of CSP A using an OTT service that may, or may not be, provided by CSP A. The OTT communication is then terminated in the US on US CSP B's network.
   In this example, CSP A may be a non-Australian entity who uses local bearers to deliver OTT services to Australians. The local carrier infrastructure owners may have the obligation to protect their network assets within Australia, effectively meeting the aims of the legislation. Again, the non-Australian portion cannot be 'protected' by CSP A as they may have no control of the networks used by the carriers bearing that communication to its destination.

3. An end user in Australia is using the internet, say to order clothes from an online store (i.e. Amazon) in Australia where the traffic routinely exits Australia to carry out routing activity and then is directed back to Australia.
   In this example, the online store's CSP providing the internet service may be a non-Australian entity who uses local bearers to deliver OTT services to Australians, or a local CSP. In either case the local carrier infrastructure owners may have the obligation to protect their network assets within Australia, effectively meeting the aims of the legislation. As in the other examples, the non-Australian portion cannot be 'protected' by local CSPs as they may have no control of any of the networks components used by the non-Australian carriers bearing that communication to its destination.

It is unclear to Industry how C/CSPs would be able to comply with their duty to do their best to protect networks that they use, given the unavoidable inability to supervise or control those networks.

The lack of clarity in the Bill raises questions in relation to this issue. For example:

Is the Bill envisaging that C/CSPs contractually require owners of all networks that a communication may use to, in turn, do their best to protect those networks? It is important to understand that such networks may be used dynamically, on an automated basis and without prior knowledge of the C/CSP on whose network the communications originated and/or without the knowledge of the C/CSPs whose networks are being used. Consequently, Industry notes that an assumption that contractual arrangements could be used to ensure

protection of networks that are being used ignores commercial and technical realities. CSPs in other jurisdictions may also not allow their national C/CSP to enter into such arrangements.

Alternatively, does the Bill envisage alternative means that would allow Australian C/CSPs to demonstrate compliance with their duty to do their best to protect networks that they use but do not own or operate? If so, Industry would be keen to understand what those means would be, how they are supposed to operate and how C/CSPs could provide proof that their compliance duty has been met.

Industry requests that the legislation should only apply to networks and facilities owned or operated under an Australian carrier licence as the ability to protect networks and facilities resides with the owner operator of that network.

3. Industry associations have raised concerns about 'acts of foreign intelligence services' in the context of whether the reforms would prevent the use of offshoring facilities and sourcing of services from non-Australian. Industry has asked whether having 'an ability to log, within Australia, any lawful access requests made to Australian systems offshore would be sufficient to fulfil the requirement of protecting networks against acts of foreign intelligence services' (pages 13 and 14, para 3.4):

    - Would your concerns about the application of the Bill to infrastructure located offshore be addressed through amendments to the Explanatory Memorandum and Administrative Guidelines to clarify whether C/CSPs would be in breach of the security obligation (section 313) if they acted in accordance with an applicable law of a foreign country?

INDUSTRY RESPONSE:

Yes. Clarification in the Explanatory Memorandum and Administrative Guidelines on the issue of outsourced or offshore arrangements will be vital for industry.

4. Industry associations suggest the term 'facilities' should be clarified. This is particularly because industry are unclear about the application of the Bill to cloud computing and particularly whether cloud computing would be captured under the definition of 'facility' in the Telecommunications Act (p16 and 17, para 3.9):

    - Would industry be satisfied if further clarifying information about the application of the Bill to cloud computing was set out in the Explanatory Memorandum and Administrative Guidelines?

INDUSTRY RESPONSE:

Yes, this would help clarify the situation around cloud computing and its variations.

Further clarification is required to the term 'facility' to exclude those facilities owned or used by a C/CSP that are not used to supply carriage services (for example, a facility used to provide content services). In the interest of certainty, this aspect may be best dealt with via the definitions in the legislation.

Notification Requirement

5. Industry associations are concerned about the existing non-exhaustive list of notifiable items outlined in the Bill subsection 314A(2)). Industry seeks that an exhaustive list of notifiable equipment be incorporated into the Bill. This is because the existing terminology implies that 'just about anything' in the course of normal network and system management must be notified. Industry says this is problematic because it is unclear what measures might be regarded as sufficient protections to meet the obligations (p14, para 3.5):

    - Can you please specify the exact level of detail you would like to see included in the list of notifiable items in subsection 314A (2)?

    - Could this be addressed through amendments to the Explanatory Memorandum and Administrative Guidelines?

INDUSTRY RESPONSE:

Industry suggests that a more specific definition of the changes that, subject to the already included test of material adversity, must be notified ought to be added into the legislation.

For example, the New Zealand *Telecommunications (Interception Capability and Security) Act 2013* (TICSA) stipulates that the changes that are to be notified are limited to "areas of specified security interest" (section 48) and the TICSA itself then goes on to list those areas (section 47).

Adding such a list to the material adversity test while also amending the legislation to only apply to networks and facilities owned or operated (but not used) under an Australian carrier licence (see Industry Response at Question 2) would make the legislation more workable, useful and practical to implement.

6. Industry associations seek that an adverse security assessment should be a requirement for the Communications Access Coordinator to provide advice on a notification (in addition to being a requirement of a direction) (p15, para 3.6):

    - Can industry please explain why specifically you consider an adverse security assessment should be required as part of the notification process?

INDUSTRY RESPONSE:

As noted in section 3.6 of our submission, the prerequisite of an adverse security assessment only applies to the directions powers of the Attorney-General but not to the assessment process by the Communications Access Co-ordinator (CAC) and the consultation process that would precede such a direction. Industry feels that there may be an inherent tendency by the CAC 'to play it safe' which may lead to an increased number of findings that a proposed change involves a risk of unauthorised interference with/access to networks that would be "prejudicial to security". (Note that the latter term is also only described in the Explanatory Memorandum instead of the legislation itself.) The lack of a formal requirement for the assessment of proposed changes allows the CAC to (intentionally or unintentionally)

apply pressure onto C/CSPs. Consequently, Industry seeks a more formal basis for the assessment of proposed changes.

International approaches

7. Industry has raised a number of concerns regarding the approach outlined in the Bill when compared to international approaches (Industry Associations p7, para 2.2). Industry Associations have noted in their submission that the telecommunications security framework adopted by New Zealand caused some companies to relocate their business operations off-shore to countries where the legislative requirements were less onerous:

    - Do you know which aspects of the New Zealand legislation, specifically, might have resulted in these companies deciding to move their business operations offshore?

INDUSTRY RESPONSE:

In 2015, the United States vendor Corse Technology, Google's research deployment at Victoria University of Wellington, the US government Energy Sciences Network in Berkley (CA), and REANNZ (a research network provider) moved a leading-edge SDN (Software Defined Network) testbed project out of New Zealand because the New Zealand *Telecommunications (Interception Capability and Security) Act 2013* (TICSA) and associated guidance material created a degree of uncertainty regarding which forms of network changes (e.g. including second-by-second network changes as they are common in an SDN world) would be covered under the TICSA.

Victoria University of Wellington noted that the testbed operators had sought clarification from the Government Communications Security Bureau (GCSB) but had not received meaningful guidance. Importantly, even though the GCSB noted that it had not requested notification to or authorisation from the GCSB for the changes in question, the uncertainty around the requirements was sufficient to move the project out of New Zealand.

This is even more alarming if viewed in an Australian TSSR context: it appears that the New Zealand TICSA is already significantly more specific regarding the changes that are to be notified than what is being set out in proposed TSSR legislation, i.e. the changes themselves are more clearly defined (Section 48 of the TICSA) and are limited to "areas of specified security interest" with those areas being listed in the legislation itself (Section 47 of the TICSA).

Australian participation in the development of 5G standards and network designs will depend on the C/CSP's ability to access SDN and NFV (Network Function Virtualisation) technologies locally. If similar restrictions are introduced under TSSR that prevent (including through the imposition of unacceptable risk to commercial entities) Australian C/CSPs from participating in the hands-on development of 5G network topologies and standards that are based on SDN and NFV, Australia will fall behind very quickly in the adoption of 5G technologies and will again be subject to the acceptance of non-Australian technology developments rather than having a seat at the table in its development.