Submission to the Attorney-General's Department on the Second Exposure Draft of the Telecommunications and Other Legislation Amendment Bill 2015

(Telecommunications Sector Security Reform) January 2016

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

18 January 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This submission is lodged by the four Industry Associations listed in the Introduction, which collectively represent the bulk of Australia's $100 billion ICT industry, including Carriers, Carriage Service Providers and Intermediaries.

The submission welcomes the fact that the Government has responded – by way of amendments - to some of the concerns raised by industry during 2015 in respect of the first exposure draft of the Telecommunications and Other Legislation Amendment Bill 2015, also referred to as Telecommunications Sector Security Reform (TSSR)).

But the submission points to continuing areas of concern with the second exposure draft, including that:

- the purpose of the proposed reform remains unclear;
- the onerous nature of the compliance requirements will act to hamper the responsiveness of carriers and carriage service providers (C/CSPs) to cyber threats;
- there remain several areas of vague drafting in the exposure draft, including uncertainty as to the status of resale of overseas services and as to the ability of intermediaries to comply with the legislation - as detailed in Section 3 of the submission; and
- the guideline information concerning the potential requirement for C/CSPs to retrofit or remove existing facilities is internally inconsistent, leaving open the risk that industry could face very high costs to rebuild existing networks.

The submission outlines the 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 and Canada. It suggests that these less onerous and less prescriptive strategies be carefully examined in Australia before proceeding down the path proposed in the exposure draft.

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 to the Attorney-General's Department on the second exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015* (second exposure draft or draft legislation, 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 Alignment of the stated purpose and the reform legislation

Industry acknowledges that Australia's critical infrastructure remains at risk from espionage, sabotage and foreign interference, including Australia's telecommunications services and networks. 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 and minimise these risks whether carried out in digital or analogue environments. 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 is 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 there is shared understanding of any potential threats and coordinated action at all levels.

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 customer trust and loyalty.

While the Associations are pleased that the revised Exposure Draft (ED) 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 proposed legislation remains of concern.

For example the revised ED now includes the ability of a service provider to make use of a Security Capability Plan, and this is an improvement. Industry considers that the fundamental approach still falls short of meeting the objective of protecting critical infrastructure from the risk of espionage, sabotage and foreign interference in the areas of:

- Onerous regulatory overhead and compliance risk,
- Excessive 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 duty for industry without an equivalent duty on the Attorney General's Department.

Industry submits that it is quick action and responsiveness that are required to strengthen network security, minimise the incidence of attacks and approach threats proactively. Industry notes also that the TSSR regime appears to be founded on the incorrect assumption that security risks are known before service introduction or equipment deployment occurs; whereas in practice, cyber threats typically emerge, or become known, after introduction/deployment. Industry's view is that the TSSR regime as set out in the revised ED does not assist the responsiveness of carriers and carriage service providers (C/CSPs) and the wider ICT industry to emergent cyber threats. But it may divert scarce resources away from investing directly in addressing cyber security threats, to compliance overhead arising from TSSR. 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 duty established in the draft legislation for the Attorney General's Department to work cooperatively with Industry in responding to threats and attacks (whereas an obligation is established in section 312 for the 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 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 be Government's intention to establish a regime of directions without evidence or corroboration of necessity.

The draft legislation, Explanatory Memorandum (EM) and the associated Guidelines still fail to answer the fundamental question of what specific failings and/or weaknesses Government is seeking to address. It remains unclear how this proposed 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 EM 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."[1]

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

The ED instead introduces a regime that imposes requirements and obligations seeking a one way flow of information from C/CSPs to Government in relation to threats to their networks and customer information. Moreover, the regime grants Government wide-ranging powers to intervene in a service provider's

- network design;
- 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.

And there is no corresponding obligation to justify Government actions, answer for the results or bear the costs. 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 Superior alternative arrangements

As outlined in the sections below, the proposed TSSR runs the very serious risk that it will not be adaptable enough to tackle the risks that will emerge. The cyber threat is 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 to be a collaborative, outcomes-focused framework. Indeed we have a proud history of working 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 proposed by the draft legislation.

[1] p. 2, para. 1, Explanatory Memorandum to the second exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*

As in the previous submission, the Associations note that in comparison to other relevant jurisdictions, the proposed legislation is out of step and over reaching. Consequently, we reiterate our concerns and point to preferred alternative approaches taken in the United States, the United Kingdom and Canada.

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 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 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. It is expected that this Executive Order will ultimately be followed by legislation by Congress.

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 cyberattacks 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.

The **UK** government has taken an entirely different approach in regard to addressing similar concerns with Critical National Infrastructure and have implemented an independent validation for vendor product security claims, noted 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. While not fool-proof, it is an approach 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 newly announced Cyber Security Growth Centre to lead this initiative and develop a collaborative environment where industry and government can work together in securing the Critical National Infrastructure programs. This new environment can be an adjunct to the TISN (Trusted Information Sharing Network) that is already established. The approach avoids the need to share confidential information with industry or the vendor, reduces the burden and cost on the Australian telecommunications sector and most importantly, it allows the Attorney General's Department to closely inspect, assess and report on any equipment that could or would compromise national security and for the vendor to respond directly to an adverse assessment bypassing the carrier altogether.

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) and that also considers 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. 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 aimed to strengthen threat protections more generally.

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, and that the Canadian Government will only impose legislation or regulation if no feasible framework can be agreed with Industry. The recent media release by the Minster of Public Safety on the Canadian Cyber Threat Strategy highlights the Canadian focus on cooperation stating that "In cooperation with provincial and territorial governments and the private sector, the Government will support initiatives and stake steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors."[2]

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 cooperation/assistance for C/CSPs to more effectively fight cybercrime.

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 considerably more expensive.

2.3 Innovation vs Legislation

Against the background of the aforementioned detrimental consequences on innovation, the Associations point out that the TSSR proposal appears to be at odds with the recently released National Innovation & Science Agenda (NISA) which sets out a whole range of measures intended to foster innovation. The NISA also 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 NISA also speaks of the intention to establish a Cyber Security Growth Centre. In this context, the European Cybercrime Strategy may serve as a model that could be adopted in a similar fashion in Australia.

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

[2] See http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

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 proposed reforms on businesses and innovation, particularly in the context of the Internet of Things (IoT).

Impact of Software Define 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 Functions Virtualisations (SDN/NFV). These technologies are at the forefront of next-generation network developments, carry functionality that is central to the development of 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 proposed 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 TICSA. (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 requests are crucial.

As the recent report IHS Infonetics, NFV Hardware, Software, and Services by analyst firm IHS 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."

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.

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 proposed reforms pose for flexible and fast innovation processes.

Given the above, the implementation of the TSSR as proposed 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 technology.

The emergence of SDN/NFV could also make the whole TSSR framework redundant. SDN/NFV separates the supply of software/functional components from hardware components and the independent sourcing/supply of such components. The risks associated with equipment supply appear to be reduced as:

I. the independence of hardware and software supply enables each layer to be protected separately; and

II. any vendor found to have introduced a vulnerability would suffer significant market loss, as it could be readily bypassed.

As there are strong indications that SDN/NFV will be the long term direction for equipment supply, evaluation of the inherent robustness of this technology approach should be completed in advance of legislative commitment to TSSR.

In light of the intended focus on innovation, collaboration and the future Cyber Security Growth Centre it appears even more the case 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 proposed 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.

Industry notes that the Cyber Security Review Report was due to be released in November 2015. Unfortunately, Industry has not received any formal information as to when it can expect publication of the report.

3. Deficiencies of the Legislation

The Associations commend Government for the revision of the first exposure draft to attempt to address a number of issues previously raised by Industry.

However, apart from the previously mentioned concerns with the general premise of the legislation, the revised draft gives rise to some new concerns and still carries some drafting concerns.

Definition of security:

Importantly, the Associations are concerned about the consequences of the introduction of the definition of security in the second exposure draft for network components and infrastructure located offshore. The revised draft legislation now ties the meaning of security to the meaning given to it in the *Australian Security Intelligence Organisation Act 1979* which defines 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".

Increasingly, these days, C/CSPs take advantage of the utility and cost effectiveness of infrastructure located outside Australia.

It is unclear how C/CSPs captured under the proposed reforms 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' 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 draft legislation (previously part of the Guidelines) as this requirement pertains to Australians and Australian networks, incl. those offshore.

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

a) preventing the use of network facilities or other infrastructure location offshore and the supply of associated services, or
b) creation of smaller scale, higher cost and delayed services using onshore infrastructure, or
c) customer migration to direct supply from offshore entities (noting for example that this is common already for social media, and social media already offers communication services, including text, voice and video).

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

It is also not clear where the boundaries between offshore activities and the resale of overseas services lie and how this would affect a C/CSP's obligations and ability to comply with them. International roaming may serve as an example, i.e. to what extent would C/CSPs be required to maintain competent supervision and effective control over the infrastructure used to supply such services?

Importantly, the proposed reforms only apply to a subset of the Australian telecommunications sector, i.e. carriers, carriage service providers and carriage service intermediaries, but they do not apply to overseas OTT services. The proposed reforms fail 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 Australian based C/CSPs, including intermediaries as defined in the *Telecommunications Act 1997 Cth* (Act). Overseas service suppliers providing OTT services will not be subject to the TSSR regime. An Australian based C/CSP simply reselling OTT services faces substantial regulatory uncertainty and regulatory risk under the proposed TSSR framework.

Industry contends that a C/CSP should only be required to take action under the proposed reform 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 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 proposed reforms, the Australian C/CSP Volptra appears likely to be prevented from supplying the email service, as Volptra cannot exercise supervision or control of the CanndyTel network (see further below). The likely market impact will be the effective blocking of Volptra (and other Australian C/CSPs) from offering the package of services available from CanndyTel.

(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 proposed reforms thus establish a lose-lose-lose outcome for Australia:

- customers lose the opportunity to deal with locally-based C/CSPs;
- Australian C/CSPs lose the opportunity to supply 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.

Intermediaries:

While the first exposure draft already included a requirement for carriage service intermediaries to do their best to protect networks from interference and unauthorised access (and thereby already created a very high bar), section 313(2B) of the second exposure draft now goes even further and requires intermediaries to maintain competent supervision of and effective control over networks and facilities.

Section 87 of the Act defines intermediaries as a person who "arranges, or proposes to arrange, for the supply of a listed carriage service by a carriage service provider to a third person (…)". On the basis of this definition it appears almost impossible for intermediaries to fulfil their obligations to maintain competent supervision of and effective control over networks and facilities which they do not own or manage in any way. The advice provided in the EM that competent supervision includes, amongst others, "the ability to detect security breaches or compromises"[3] and that effective control "means the ability of the C/CSP to maintain direct authority and/or contractual arrangements which ensure that its network and facilities, infrastructure and information stored or transmitted within, is protected from unauthorised interference. This would include authority over all parties with access to network infrastructure and data"[4] simply ignores the technical and commercial realities of intermediaries.

To the extent that the obligations of the draft legislation are able to be applied to intermediaries, they need to be amended to reflect intermediaries' abilities to actually protect information that is carried by a communication that they arrange.

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 proposed regime and will leave them at a

[3] p. 24, para. 109, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*
[4] p. 24, para. 110, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*

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, (as in the previous exposure draft) section 315B 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 second exposure draft now includes the requirement that such a direction by the Attorney-General must only be given after an adverse security assessment in respect of the C/CSP has been given to 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 on 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 draft 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 the 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 EM[5].

Notification requirements:

Section 314A of the revised draft provides that C/CSPs must notify the Communications Access Co-ordinator (CAC) if they become aware that the implementation of a proposed change to a service or system is likely to have an adverse material effect on that C/CSP's ability to comply with its security obligations. The draft legislation then (non-exclusively) lists a number of events that are considered changes and that <u>may</u> give rise to a negative assessment by the C/CSP. This approach is reasonable as C/CSPs have extensive and rigorous practices and processes in place to assess security risks for systems and network changes and, consequently, will be able to identify the level of risk associated with the proposed change. Where they identify an adverse material risk, C/CSPs will then notify the CAC as required by the draft legislation.

[5] p. 14, para. 62, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*

Unfortunately, the revised legislation is at odds with the EM which states that the "New section 314A of the Telecommunications Act outlines the types of changes in arrangements that should be notified to the CAC, which include but are not limited to: (….)."[6] The EM should be amended to reflect the drafting of the legislation.

Old vs. new networks and facilities:

Section 313(1) as drafted 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.

The draft Guidelines attempt to provide further guidance on this issue, but are, unfortunately, internally inconsistent.

The Guidelines state that "While the security obligations will have immediate effect from the expiry date of the implementation period, existing systems, networks and facilities in place at the time the security obligation comes into effect that are non-compliant will not be penalised."[7]

The Guidelines go on to state, however, that C/CSPs "are not expected to retrofit all systems on commencement of this security obligation, except in very rare cases (…)."[8]

Given the very high bar placed by the new 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 administrative guidelines that non-compliant systems will not be penalised does not create sufficient certainty for C/CSPs (particularly when such assurance is immediately contradicted in the guidance provided).

At the very least, the draft legislation ought to be amended to reflect this intention (not to require retrofits except in rare 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 are willing to continue to engage with Government, Parliamentary Committees and individual political representatives on the mutual desire to ensure the robustness of national communications infrastructure and to devise appropriate tools to further that aim.

However, as evidenced in this submission, the Associations believe that the draft legislation is unnecessary and in its current form still too discretionary and vague.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

cc:
Minister for Communications, Senator the Hon Mitch Fifield

[6] p. 25, para. 19, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*
[7] p. 25, *Telecommunications Sector Security Guidelines*, draft version November 2015.
[8] p. 25, *Telecommunications Sector Security Guidelines*, draft version November 2015.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507