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

(Telecommunications Sector Security Reform)
July 2015

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

27 July 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As has been stated in previous submissions[1] to Government, the Associations acknowledge Government's desire to protect telecommunications infrastructure and the information transmitted across it from unauthorised access and interference. Indeed, Australian Carriers, Carriage Service Providers and Carriage Service Intermediaries (C/CSPs) and other industry participants have an active and vested interest in ensuring that the nation's networks and communications infrastructure are robust and resistant to external attack.

Industry is, however, unable to support the proposed Telecommunications Sector Security Reform (TSSR), as described in the exposure draft legislation, for reasons including that it constitutes regulatory 'over-reach' in the form of a framework that:

- will face challenges protecting communications networks, i.e. it will not deliver the increased protection the proposed reforms are aiming to achieve;
- is out of step with regulatory approaches to protecting networks adopted in other countries, including the UK, USA and Canada, thereby putting Australia at a disadvantage in fighting cyber threats and undermine Industry's ability to support these important peers;
- hands unjustifiably significant additional and intrusive powers to Government and places regulatory burdens on Industry that will undermine its ability to protect against and respond to cyber attacks;
- risks being highly disruptive to the deployment of new network technologies that are more robust in preventing cyber attacks;
- will be a significant deterrent to technological investment in Australia;
- imposes additional costs on Industry and (ultimately) consumers undermining Australia's competitiveness at a time when digital innovation is an important area for growth for Australia;
- fails to offer protection/indemnity to C/CSPs against the risk of civil litigation through 'safe harbours', thereby limiting information sharing and the ability to quickly respond to threats and to jointly engage in preventative action;
- carries the risk that competition in infrastructure supply will be reduced, to the detriment of all Australians;
- lacks transparency; and
- fails to provide adequate consultative mechanisms and avenues of appeal.

Industry also notes that the revised version of the Australian draft Guideline associated with the proposed legislation has not been made available to Industry as part of the exposure draft consultation. It is imperative that this revised Guideline be available for scrutiny and debate before the Government attempts to takes any further steps in relation to the draft legislation.

The Associations are also concerned by the ongoing costs associated with the introduction of this regime and the additional red-tape it will introduce. These costs will be added to the already substantial imposts placed on Industry as a result of recent Government initiatives in the form of the mandatory two-year data retention scheme, online copyright notice scheme and the newly-legislated piracy website-blocking regime.

Industry is not convinced that Government, security agencies, Industry or the Australian public will derive significant benefits from the proposed reforms that would justify the intrusion

[1] For example: Proposed regulatory scheme to enhance the security, integrity and resilience of Australia's telecommunications infrastructure, March 2012; Submission to the PJCIS, August 2012; Submission to the Consultation on Draft Guidelines to inform Government's consideration of the Telecommunications Sector Security Reform (TSSR), May 2014 and March 2015; and Submission to the Department of Prime Minister and Cabinet Cyber Security Review Consultation Paper, April 2015

into the commercial operations of Australian C/CSPs and the attendant compliance costs. The additional costs of compliance may also make Australian based C/CSPs uncompetitive in the delivery of infrastructure and services to the global telecommunications market, including multinational corporations.

In fact, the Associations see the very real danger that the proposed reforms will mean a step backwards in dealing with cyber threats and breaches as they will divert resources from investing in addressing cyber security threats to compliance with onerous obligations and reduce the ability for the ICT industry and its clients to proactively monitor and quickly respond to threats and breaches.

The Associations remain concerned that the introduction of the proposed framework will militate against the current cooperative and collaborative flow of information between C/CSPs and security agencies – a framework that (while potentially leaving room for improvement) Industry believes operates efficiently in its current form.

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 a submission to the Attorney-General's Department on the exposure draft *Telecommunications and Other Legislation Amendment Bill 2015* (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. General Observations

2.1 Unclear purpose of the framework

Industry understands Government's desire to protect and minimise the impact of cyber threats from malicious actors and state-sponsored attacks. Industry also agrees that an overarching cyber security framework is necessary.

However, as noted in previous submissions, it appears that the Explanatory Memorandum (EM) or other documents in relation to the draft legislation still do not adequately address some underlying key questions. In particular:

- What specific failings and/or weaknesses is Government seeking to address via its proposed TSSR reform package?
- How will the information Government is seeking be used to minimise the threat of espionage, and further, what is the perceived connection between the risk of espionage and the security of telecommunications infrastructure?
- How does the introduction of the proposed regime benefit the current cooperation between Industry and security agencies in relation to information flow and notification of security risks?

The Associations fail to see any evidence that the current legislative regime is deficient. The reforms appear to be premised on an assertion that the current legislation is deficient and does not reflect national security concerns. The main thrust for this assertion appears to be that the current legislation does not provide sufficient granularity of power for authorities and agencies to give flexible directions to C/CSPs, i.e. that it only enables 'all or nothing' responses. Furthermore, there appears to be a view that the current legislation is unworkable or not useful, simply because certain powers have never been exercised.

The EM broadly describes the aim of the proposed regulatory framework as the "promotion of risk-informed management of national security risks in the telecommunications sector".[2] The EM also notes the "networks and infrastructure of carriers, carriage service providers and carriage service intermediaries (C/CSPs) have become attractive targets for those who wish to harm Australian interests"[3] and that technological advances have introduced significant vulnerabilities to networks and critical infrastructure.

The Associations contend that the proposed reforms do not constitute or contribute to a meaningful national cyber security framework and will not deliver the stated aim. Instead the draft legislation introduces a regime that places significant obligations on C/CSPs to provide information to Government about activities being conducted on their networks and grants Government wide-ranging powers to intervene with network design. This will significantly slow down the responsiveness of C/CSPs and the wider ICT industry to cyber threats. However, such quick action and responsiveness are required to strengthen network security, minimise the incident of attacks and approach threats proactively.

Compounding this risk is the absence of clear arrangements in the draft legislation for Government to work cooperatively with Industry in responding to threats and attacks. Consequently, Industry is concerned that its ability to effectively isolate cyber threats and minimise disruption will be significantly diminished.

[2] p. 2, para. 4, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*

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

2.2 Overseas approaches and experiences

The Associations note that in comparison to other relevant jurisdictions, the proposed legislation is out of step and more far-reaching.

Industry firmly believes that joint Industry and Government fora for sharing cyber security activity and methods to deal with such activities constitute a more effective and responsive way to deal with cyber threats. Such a collaborative approach has been adopted by the UK, USA and Canada. Industry strongly recommends Australia embrace a similar approach to ensure that Industry is able to quickly deal with network vulnerabilities and to foster innovation. Industry contends that the proposed reforms will slow down responsiveness and stifle innovation.

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.

Against this background, the Associations reiterate that a more sensible approach would be to reconsider the roles and responsibilities around the sharing of information about actual and potential threats, and what tools and techniques are recommended to ensure appropriate action is taken to protect networks. To achieve this the development of suitable fora that encourage Industry and Government disclosure of such information is 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.

As previously submitted, to ensure business is encouraged to voluntarily disclose threat and attack information with Government and third parties, 'safe harbour' arrangements similar to those in the USA are required to ensure C/CSPs are not exposed to potential legal action for sharing information. The 'safe harbour' can also protect the information from being used by agencies to regulate other activities.

It is imperative for Australia to leverage the important activities undertaken in the USA and elsewhere and to adopt, as much as possible, global standards. This will enable Australia to work more effectively in concert with key global jurisdictions, and ensure technology that is developed to address threats is consistent across the globe.

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

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.

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.

While the New Zealand *Telecommunications (Interception Capability and Security) Act 2013* (TICSA) has significant shortcomings (see below), it appears more reasonable and practical than what is being proposed for Australia. The TICSA is similar in some respects to its proposed Australian counterpart, however it does set practical limits on what C/CSPs must provide to the NZ Government Communications Security Bureau (GCSB), by specifying areas of security interest rather than employing a broad catch-all approach. Notably, the NZ framework does not mandate specific measures as to how to secure a C/CSP's network. Industry also notes that the GCSB has the power to grant class-order exemptions for particular activities and, indeed, has granted such exemptions.

Even though the TICSA is less discretionary than its Australian counterpart, NZ C/CSPs find the scheme a significant administrative burden with preparation for notifications taking up to several days. Importantly, the NZ experience shows that the TICSA has introduced a major element of uncertainty for businesses and introduces unnecessary practical difficulties. For example, C/CSPs are faced with a balancing act to find the 'optimal' notification time slot: where C/CSPs notify authorities too early in the sourcing process, vendors or requirements may not have been locked down and it is impossible to provide the required details to authorities. If C/CSPs wait until these issues have been finalised, a commercial 'point of no return' is reached and any deviating request from authorities, if at all, can only be addressed with a negative financial impact on the project. Section 2.3 of this submission explores other negative consequences of the TICSA which would be equally likely to materialise in Australia under the proposed TSSR.

Importantly, C/CSPs in NZ report that they genuinely do not see any real evidence of clear benefits to Government or Industry from the introduction of the TICSA. To the extent that the TICSA results in marginal benefits by driving better risk management and security policies in smaller CSPs, who previously may not have had informal relationships with the relevant agencies, it can be argued that – given their equally marginal contribution to nationally significant services or infrastructure – the costs and risks to investment of the framework far outweigh its benefits.

2.3 Consequences for business and innovation

Importantly, 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 in the best position 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 increased sophistication of cyber threats. Businesses will focus on minimising exposure to regulatory imposts or on compliance instead.

Such 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 Internet of Things (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 struggle to understand very new technologies and their use within networks and, as a result of this inexperience and lack of expertise, may 'err on the side of caution' and deny implementation.

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."[4] 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."[5]

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.

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.

Industry is aware that, during recent Parliamentary debate on the data retention legislation, a potential amendment to the TSSR legislation was flagged that would mandate that data retained pursuant to the data retention regime be stored onshore, i.e. within Australia.

There is a range of views among Association members (some of whom operate data centres in Australia) on the potential requirement. One view is that the underlying notion that data stored onshore is per se more secure than if stored outside Australia may be naïve, incorrect and ignores the technical realities of cyber threats. Not the location of the data but rather the policies and procedures in place to protect it define the security of data. Such a requirement, if enacted, would pose additional costs and significant difficulties for many C/CSPs and is likely to drive businesses out of Australia.

The EM correctly observes that "It is a commercial reality that most C/CSPs will already have some component of outsourcing and offshoring in their business service delivery and support models"[6] and goes on to say that "The reform is about establishing mechanisms to identify and appropriately manage risks associated with these business delivery models."[7] Industry is heartened by these statements and the Government's reassurance in the EM that the "security framework is not about preventing the use of particular equipment vendors or service suppliers".[8]

Unfortunately, however, there is nothing in the legislation that prevents Government from taking arbitrary decisions to exclude any equipment vendor it so chooses from participating in the Australian market. Misuse of such power could fundamentally diminish competition in Australia, bringing a range of poor outcomes that might include higher prices, sub-optimal services and reduced opportunities for investment and employment.

On the other hand, there are important considerations such as jurisdictional enforcement and the protection of privacy and personal information of Australian citizens. The Associations welcome further discussion on these issues.

[4] Quote taken from CommsWire Daily, 20 July 2015, *NFV MARKET TO GROW 500% IN FOUR YEARS*
[5] Quote taken from CommsWire Daily, 20 July 2015, *NFV MARKET TO GROW 500% IN FOUR YEARS*
[6] p. 3, para. 8, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*
[7] p. 3, para. 8, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*
[8] p. 3, para. 8, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*

2.4 Vague and discretionary legislation

Industry objects to the proposed legislation as it is vague, overly broad and delivers undue discretion to Government. Section 315B, which allows the Attorney-General's Secretary to give "a written direction requiring the carrier, provider or intermediary to do, or to refrain from doing, a specified act or thing within the period specified in the direction"[9], may serve as only one example of the wide-ranging and open-ended nature of the draft legislation.

Moreover, the decision-making thresholds for the Attorney-General or the Attorney-General's Secretary exercising their directive powers set out in the new section 315 are very low. The legislation is lacking notification and consultation obligations and, alarmingly, does not grant an 'administrative appeals' process.

Discretionary powers:

The new Section 315C provisions allow for the request of information from the Attorney General's Secretary in particular form and without the option of non-compliance, regardless of the sensitivity of the information or the potential for self-incrimination of the C/CSP when providing the information.

Section 315G allows delegation of powers to the Australian Security Intelligence Organisation (ASIO) or a Senior Executive Service officer in the Attorney-General's Department and provides that, once documents are supplied, they can be kept as long as desired and be shared with anyone deemed to have a role in considering the relevant security issue. This will not appropriately protect commercially sensitive data. The Associations recommend a more narrowly defined circle with whom the provided information can be shared.

Overall, the draft legislation also does not appear to provide sufficient detail as to when the Attorney-General's powers can be applied, and the response timeframes for C/CSPs to requests they may receive.

Section 315A(1)(b) provides that "the Attorney-General, after consulting the Prime Minister and the Minister administering this Act, considers that the proposed use or supply (of a carriage service) would be, or the use or supply is, as the case may be, prejudicial to security; the Attorney General may give the (C/CSP) a written direction not to use or supply, or to cease using or supplying, the carriage service or the carriage services."[10]

Section 315B extends similar powers to the Attorney-General's Secretary, i.e. all it requires to allow for a direction to be given is that the Attorney-General's Secretary is satisfied that a risk of unauthorised interference with, or unauthorised access to, telecommunications networks or facilities exists, and, as a result, there is a risk to security.

In both cases, there is no qualification of the threat or risk assessment used to justify action. As drafted, if a threat or risk merely exists, it may provide an adequate basis to proceed. This provides a very 'low bar' for the exercise of these powers.

The Associations request that the decision-making threshold be further qualified, such that the basis for action is that the identified risks or threats must exhibit characteristics, for example, they must be:

- imminent;
- substantial;
- likely;
- identifiable;
- known;

[9] Section 315B(1), exposure draft *Telecommunications and Other Legislation Amendment Bill 2015*
[10] Section 315A(1), exposure draft *Telecommunications and Other Legislation Amendment Bill 2015*

- feasible (technically or commercially);
- of severe potential impact.

Unless the benchmark for directive action is made more rigorous, decision-makers have virtually unfettered discretion, because every deployment or business process will have some level of identifiable risk or vulnerability. Conceivably, any risk can be made to relate to security as there is inevitably some relationship to live network traffic, customers or service information which can be extrapolated and deemed sensitive.

Notification, consultation, review and appeals:

Procedural fairness would ordinarily dictate that the intended recipient of an adverse finding or action (such as a direction) would be notified in advance and have an opportunity to provide a final argument to the decision-maker. In this context Industry notes that the EM contains an intention that "C/CSPs will be given sufficient notice of the intent to use the directions power to enable representations to be made about the proposed direction."[11] However, this notification process is not reflected as a requirement in the actual draft legislation.

Section 315B contains the provision for consultation with the Director-General of Security and the Communications Secretary (and other optional parties) prior to a direction being given to a C/CSP. Industry notes with great concern that the draft legislation does not include an obligation for consultation to be undertaken with the concerned C/CSP prior to any of these events occurring.

Importantly, the Associations are alarmed by the lack of an 'administrative appeals' process (i.e. under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act)) for decisions made under the new sections, e.g. appeals against injunctions and enforceable undertakings for breaches of the new provisions in the *Telecommunications Act 1997* (Act). Given the severe penalties associated with non-compliance, an 'administrative appeals' process is imperative. A mere judicial review of the decision making process is not sufficient. A review mechanism of the merits of a decision is required.

It is also noted that as per the *Australian Administrative Law Policy Guide* issued by the Attorney-General's Department "Exclusions from the application of the ADJR Act are rare and will only be considered for compelling policy reasons."[12] The Associations point out that the mere fact that the matter at hand broadly concerns national security does not necessarily constitute a "compelling policy reason".

Assertions that the powers granted to the Attorney-General's Department would only constitute measures of 'last resort', while perhaps intended to provide a degree of reassurance, do not provide a legal basis upon which C/CSPs can rely when the need for such intervention is in dispute.

The only reviewable element in the current proposal is the ASIO risk assessment, which can be reviewed by the special 'security' Administrative Appeals Tribunal. While this affords an avenue to engage, it has significant shortcomings: it does not directly relate to the maker of the direction nor the decision, and there is no requirement for any re-consideration of the direction if the Tribunal does find a point of disagreement with the ASIO security assessment.

2.5 Compliance and enforcement

The EM notes that "Under the proposed framework, Australian Government agencies, (in particular the Australian Security Intelligence Organisation (ASIO)) would provide general and targeted threat assessments and mitigation advice to C/CSPs to manage risks to their

[11] p. 21 Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*
[12] pp. 14/15 Attorney-General's Department *Australian Administrative Law Policy Guide*, 2011

networks. Administrative guidelines are also to be developed to assist C/CSPs to understand what parts of networks are particularly vulnerable to unauthorised access and interference, and provide guidance on the controls and measures that can be implemented to manage these vulnerabilities."[13]

The Associations are unable to locate the section of the draft legislation which would reflect the above statement. Industry is uncertain as to how and when a C/CSP can expect to receive the aforementioned ASIO assessments.

While the Associations agree with the principle of guidelines to contain the specific practical details to assist C/CSPs with understanding the legislation and what precisely is required of them, it should also be noted that C/CSPs themselves have a significant commercial interest in minimising and managing the risks to their networks.

The impact and response to the legislation will be influenced by the interpretation and expectations contained in the Guideline as is the case with the New Zealand TICSA guidelines which provide practical guidance and examples to support C/CSPs to comply with the legislation. Similarly, the current discussions in the wake of the new data retention regime clearly highlight the need for practical and timely guidance C/CSPs can use to ensure they comply with demanding new legislation.

Unfortunately, the Australian draft Guideline made available to Industry earlier in 2015 is now to be superseded by a new version, but this new version has not yet been sighted by Industry and – as we understand it – will not be available before the deadline for submissions in response to the exposure draft legislation. It is therefore impossible to comment on the guidance that may be available through the Guideline. It is imperative that this revised Guideline be available for scrutiny and debate before the Government attempts to takes any further steps in relation to the draft legislation.

The Associations remain concerned with the lack of specificity of the draft legislation and associated documents regarding the network parts that are of greatest concern to Government and the information to be supplied by C/CSPs, i.e. it is unclear which parts of a network would be classified as "sensitive", what constitutes a "sensitive business activity" and what qualifies as a "key network development". The unavailability of the revised Guideline make it impossible to assess if these issues would be addressed to Industry's satisfaction.

In the same vein, it is not clear to Industry how C/CSPs will engage with authorities. The Regulatory Impact Statement (RIS) indicates that C/CSPs could be assigned a level of priority ("low priority" vs. "high priority"). However, it remains unclear how the level of priority would be determined or what obligations apply based on this determination. The RIS also fails to set out avenues for challenging or altering a classification that has the potential to cause severe commercial damage to a C/CSPs through a reduced ability to compete for private or public ICT contracts. Industry also wishes to highlight that networks comprise owned and leased/licensed components, and network components as well as their ownership change over time, thereby contributing to the complexity of the issue.

The draft legislation also gives rise to additional problems for C/CSPs whose head office may be located outside of Australia. Often the release of the information required by authorities is dependent on the decisions of the C/CSP's head office and such commercially sensitive data may need to be discussed on an internal basis weeks (or even months) before it may be approved for external release.

Moreover, given the very wide scope of directions, it is possible that in complying with a direction, C/CSPs may find themselves unable to comply with another regulatory requirement such as the Universal Service Obligation, a Structural Separation Undertaking or the Customer Service Guarantee. For example, a C/CSP may wish to upgrade a particular piece of infrastructure to ensure compliance with other regulatory requirements but may find

[13] p. 3, para. 7, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*

that a direction made under the TSSR legislation obstructs that C/CSP's capacity to (continue to) meet those requirements.

In the context of mobile telecommunications, the Associations would like to draw attention to the use of the terms "unauthorised access" and "unauthorised interference". Whilst the EM states that for the purposes of Section 313, these terms should be understood according to their ordinary meaning and use, these terms may in fact have a different meaning in relation to telecommunications (e.g. mobile and wireless) networks than in a national security context.

As set out in previous submissions, the Associations note the lack of an overarching cyber security framework developed prior to the implementation of its components such as the data retention regime or indeed the TSSR proposals. 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.

For example, the EM states that the Parliamentary Joint Committee on Intelligence and Security "recommended that the government enact the proposed telecommunications sector security reforms prior to the end of the implementation phase of the data retention regime."[14] However, Industry notes with worry that the enactment of the TSSR will impact C/CSPs' timeframes for implementation of network changes. When submitting Data Retention Implementation Plans (DRIPs) C/CSPs would either not have accounted for potential delays due to TSSR notification processes or, if taking those into account, they will not be able to include meaningful timeframes in their DRIPs as required by the data retention legislation. As a result C/CSPs may be faced with a potential breach of their obligations.

2.6 Costs and timeframes

Industry is aware that improved infrastructure security may have qualitative factors associated with it that are difficult to quantify but note that it is uncertain which benefits may derive from the proposed regime. As submitted, Industry does not believe the proposed reform will necessarily produce improved infrastructure security.

Assertions that additional intelligence currently unavailable to Industry would be made available under the new regime are difficult to assess – if intelligence agencies hold information concerning potential threats at present and do not pass these on to Industry, then that would appear to point to deficiencies in practices by the agencies rather than by C/CSPs.

While the Associations are pleased that the cost-recovery model previously proposed to be borne by Industry has not found its way into the current draft legislation, Industry reiterates its concerns about the ease with which incremental costs appear to be applied to Industry through a raft of legislation and/or regulation (i.e. data retention legislation, copyright regulation and piracy website blocking legislation, TSSR and cyber security reform) – all without a clearly formulated view from Government on an overall strategy or a discussion on a sensible funding contribution model.

The Associations also reiterate that the implementation timeframe – to be specified in the legislation – ought to be greater than 12 months to allow for the consideration of normal financial/business and approval cycles. Industry continues to consider any shorter timeframes unrealistic, especially in light of the (equally too short) 18 months implementation timeframe for the data retention regime.

Against this background, Industry is very concerned that the draft legislation does not even contain a minimum 6 months implementation timeframe but rather refers to a "day fixed by

[14] p. 7, Para. 7, Explanatory Memorandum to the exposure draft of the *Telecommunications and Other Legislation Amendment Bill 2015*

Proclamation".[15] Industry notes that the mere intent to grant a 6 months implementation period as laid out in the EM does not provide an acceptable degree of certainty for C/CSPs.

3. 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.

As evidenced in this submission, however, the Associations do not believe that the draft legislation is proportionate or appropriate and the Associations strongly urge all sides of politics to undertake a 're-think' – and detailed discussions with industry – before proceeding down a path that will be, on balance, detrimental.

Industry also looks forward to receiving the draft Guideline in the near future to gain a better understanding of the proposed requirements of the draft legislation and the practical implications it will have for C/CSPs in Australia.

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, The Hon Malcolm Turnbull MP
Parliamentary Secretary to the Prime Minister, The Hon Christian Porter MP

[15] Item 2 Commencement, exposure draft *Telecommunications and Other Legislation Amendment Bill 2015*

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 9
32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507