Australian Attorney-General's Department

Consultation on Draft Guidelines to inform Government's consideration of the Telecommunications Sector Security Reform (TSSR)

Submission as prepared by:

Communications Alliance
and
Australian Mobile Telecommunications Association

6 March 2015

Executive Summary

Communications Alliance and the Australian Mobile Telecommunications Association (the Associations) welcome the opportunity to comment on the Attorney-General's Department's (March 2015) consultation on its Telecommunications Security Sector Reform (TSSR) proposals, draft Guidelines and proposed cost recovery arrangements.

As has been stated in previous submissions to the Government (*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)* the Associations acknowledge Government's desire to protect telecommunications infrastructure and the information transmitted across it from unauthorised access and interference.

However, the Associations remain concerned that key questions around the threats that the proposed reform intends to address, the desired outcomes and the connection between perceived threats and telecommunications infrastructure, remain unaddressed.

Furthermore, the Associations observe that the lack of specific information from Government so far (e.g. regarding which network components would be deemed critical and which business activities are considered sensitive) makes an assessment of the viability, proportionality and usefulness of the proposed measures very difficult. The Associations also seek further clarity on the proposed compliance framework and the mechanism by which providers will be asked to demonstrate compliance with the framework.

Importantly, the Associations continue to strongly oppose the cost recovery model put forward by Government, which burdens Industry with significant additional costs that ought to be borne by the law enforcement agencies seeking the legislative and regulatory change. Industry is yet to be convinced that it derives significant benefits from the proposed reform that would justify such a transfer of cost impost.

1. Introduction

The Associations

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, carriers, carriage and internet service providers, content providers, search engines, 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, see http://www.commsalliance.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 (CSPs), handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry. For more details about AMTA, see http://www.amta.org.au.

In this submission the Associations will provide comments on the paper *Telecommunications Sector Security Reform, Attachment A* (Consultation Paper) and the guiding principles of the Government's *Guidelines for Carriers, Carriage Service Providers and Carriage Service Intermediaries, Attachment B* (Guidelines) on the Requirement to Protect Telecommunications Networks and Facilities from Unauthorised Access and Interference, and the associated proposed cost recovery model.

2. General Observations

Purpose and Context of the Framework:

While the Associations are pleased to note that the recent Consultation Paper contains more details around the envisaged legislative amendments and enforcement mechanisms, there remains a level of concern that some underlying key issues have not been clearly articulated. In particular:

- What failings and/or weaknesses is Government seeking to address via its proposed TSSR reform package?
- What are Government's desired outcomes?
- 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?
- What is the relationship between the proposed Telecommunications Security Sector Reform (TSSR), existing engagement frameworks and other security-related policy reviews on foot?

The Guidelines describe the purpose of the framework as to "appropriately safeguard core and critical components […] as a means to more effectively counter threats to security through the supply of equipment and managed services, in particular first order threats such as espionage via cyber means or attacks on systems underpinning critical infrastructure". Industry seeks more specific details as to the threats of most serious concern. It also remains unclear why the focus appears to rest on "equipment and managed services" and in what way these are distinct from the data security/malware/hacking threats that are of common concern to all businesses that are IT reliant. In this context, Industry emphasises that recent data breaches such as the well-publicised Sony Pictures and Apple iCloud hacking scandals – which form the most common threat to data transmissions and storage – are not provider-related but occur at the customer end of the communications. Industry is concerned that there is an implicit notion that the proposed framework ought to assist with addressing this kind of data hacking.

The Associations remain concerned with the lack of specificity of the Consultation Paper and Guidelines regarding the network parts that are of greatest concern to Government and the information to be supplied by providers, 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"? Furthermore, the Consultation Paper does not contain sufficient detail regarding the TSSR Engagement Process (as depicted in the Paper's diagram), i.e. it does not elaborate on how a provider's priority ("low priority" vs. "high priority") is determined or what obligations apply based on this determination. 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.

Looking at a wider policy context, the Associations are keen to understand the relationship between Government's Telecommunications Security Sector Reform (TSSR) and the Cyber Security Reform efforts currently also being undertaken by Government. It appears that the logical chronological order of actions has been reversed, i.e. elements (TSSR) of a larger strategy are being considered before the strategy itself (Cyber Security Reform) has even been defined.

In addition, it is unclear how an additional TSSR engagement framework relates to the broader Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience. The TISN encompasses other essential services sectors, including banking and finance, energy, transport, health, water and food, not just communications, which enables cohesive

engagement and sharing of information between business and government on critical infrastructure security issues and continuity of service across all of these essential services.

Current Engagement:

Industry concurs with the view that carriers and security agencies have cooperated effectively in the management of security risks that relate to telecommunications infrastructure operated by Australian providers. However, Industry does not entirely agree with the characterisation of all engagement between the parties as informal. Numerous interactions occur on the basis of formal rules. Yet in cases where no formal rules of engagement have been used, the absence of a formal security framework has largely contributed to a frank discussion and a good flow of information between the parties. Industry is concerned that the introduction of a regulatory security framework may contribute to a more restrained flow of information as providers must fear that the information they provide will be subject to regulations and potential enforcement action or even penalties.

Compliance and Enforcement

While the Consultation Paper includes more detail around the enforcement powers and notification requirements, the Associations would like to gain a better understanding if it is proposed that Industry work with Government on the security framework or if it is proposed that providers achieve a level compliance with or certification to a standard. If the latter is the case, is it envisaged that compliance be audited and if so through what authority (e.g. external auditors)? It is also not quite clear what ramifications a data breach would have for a provider that has complied with the framework.

The Consultation Paper proposes to vest the Secretary of the Attorney-General's Department with certain enforcement/direction powers. Industry contends that there is merit in considering a co-ownership of those powers, e.g. with the Secretary of the Department of Communications, to ensure greater independence.

Cost Recovery and Implementation:

With regards to the proposed cost recovery model, Industry's remains strongly opposed to any proposal that shifts the costs of the regime to Industry through whatever mechanism. Industry contends that agencies should assume cost responsibility – and at the very least, responsibility for their own costs – where it is law enforcement and national security agencies that are requesting amendments to regulations.

In keeping with best business practices, any expenditure needs to be evaluated against the potential benefits that it might bring. Industry is aware that improved (provided the proposed measures result in an improvement) infrastructure security may have qualitative factors associated with it that are difficult to quantify. However, a more detailed articulation of the immediate infrastructure risks is necessary so that the measures being proposed can be evaluated within that context, rather than within the context of a governmental desire to future-proof networks against threats as yet unseen. This would allow both Industry and Government to evaluate if the measures are proportionate to the envisaged risks.

The Associations note that Industry is uncertain which benefits it may derive from the proposed regime. Assertions that additional intelligence currently unavailable to Industry would be made available under the proposed regime are difficult to take into consideration as potential benefits to Industry without further details or examples of such information.

Even if Industry was willing to accept a cost impost, it is unreasonable for Government to expect Industry to also pay approximately $2m per annum in additional headcount and other

costs that Government proposes to spend within the Attorney-General's Department and security agencies. The Associations are also keen to understand the breakdown of the above costs estimate which appears to remain unchanged (at a high level) despite a contingency fund of $500k no longer being included in the estimate (as verbally indicated by the Government).

Industry notes that the recent Consultation Paper still assumes that an appropriate implementation timeframe could be around six months. The Associations reiterate that this timeframe is not realistic as it neglects considerations of normal financial/business and approval cycles of at least 12 months or more that providers must go through to secure funding for changes to business processes or network components.

3. Guiding Principles and Suggested Controls

With regards to the Guiding Principles and Suggested Controls, the Associations re-iterate the specific concerns and questions raised in our previous submission as it appears that they have not been addressed in the most recent draft guidelines.

Industry is particularly concerned with the proposed reliance on an ITU standard. Instead Industry considers that the development of an Industry guideline, developed in consultation with Industry would provide a more viable and efficient alternative.

Principle 1

Assets should be identified and an inventory developed and maintained

Control: ITU-T Rec X.1051 –paragraphs 4.2.3, 7.1, 7.2

The Associations seek clarification on Government's understanding of the term 'critical infrastructure'. Infrastructure at the consumer level is unlikely to carry a similar level of risk to national security as would, for example, a government network such as the Department of Defence. In addition, Industry seeks an indication of the drivers behind this requirement, thus allowing for consideration of the merits of including items such as utilities and organisational reputation on a list designed to ensure network security in the national interest.

With regards to the assets listed in the ITU-T Rec. X.1051, Industry notes that providers already have processes in place for identifying and recording network elements for financial purposes. To conduct a similar exercise for Government for the purpose of identifying security critical network elements would represent a significant impost on providers that would appear to be unwarranted given the existence of standard asset inventories, the contents of which may well satisfy Government's specific requirements. It is also noted that in instances where infrastructure may be housed in leased premises, providers are likely to have little control over security mitigation measures that might be in place for elements such as air conditioning or heating.

An alternative approach to a default deferral to the ITU standard might be the development of an Industry guideline, developed in consultation with Industry, which would provide Industry players with a more specific list of the relevant network elements which are deemed to be critical to infrastructure security.

Principle 2

Assessments of risk should be ongoing to ensure security measures align with change.

Control: ITU-T Rec X.1051 – paragraphs 4.2.3, 4.2.4.2, 7.1 and 7.2.

While the Associations acknowledge the importance of assessing risk levels in establishing a form of standardised network resiliency measure, it would seem reasonable that a consistent approach be applied to both private sector and critical government infrastructure.

The Associations note that there are also other non-infrastructure related risks to providers:

- the potential for the proposed regime to bring providers into conflict with existing corporate regulations, particularly those relating to the disclosure of information;
- the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
- impacts on competition in the market-place and risk that proposed requirements may create a barrier to entry for new, lower cost providers and could eliminate some of those already in the market, resulting in decreased market competition on pricing and general consumer detriment;
- the absence, to date, of any protection/indemnity to civil action for providers who have acted in good faith under the requirements of the proposed amendments;
- the fact that the rapidly changing technology landscape, where potential vulnerabilities now exist at the physical, network and application layers, has not been sufficiently taken into account, specifically with regards to the concept of 'critical infrastructure'. Certain threats may be specific to particular systems at a single layer, whilst others may impact multiple systems across all layers; and
- the potential for overlap with existing corporate and sector specific regulations. Organisations currently have responsibilities about reporting major corporate actions, e.g., mergers and acquisitions, under various corporate regulations. The reporting processes to Government that are being proposed may require earlier disclosure of such information than would be normally triggered for these corporate regulations.

With regards to the risk assessment being an ongoing requirement, the Associations draw the Government's attention to the significant allocation of resources and costs that would be required to capture all identified risks in a single document.

Principle 3

Engage with Government to identify and mitigate security concerns more effectively.

Control: ITU-T Rec X.1051 – paragraph 6.1.6

The Associations concur with the Government that network security and resilience are important in the digital age and that close cooperation between service providers and Government is necessary for exchange of information and possible threats observed.

Before practicable solutions on security issues can be developed both Industry and government would benefit from the real time identification and assessment of risks and threats that have the potential to compromise network security and resiliency and to put customers at risk. The Associations note that there are facilities/bodies in place which could play key roles in the proactive identification and notification of network impacting threats, those being the Cyber Security Operations Centre (CSOC), Cert Australia, the Australian Signals Directorate (ASD), the Australian Cyber-Security Centre and the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience. Yet at this time it is unclear as to the remit of each of these instruments with regards to threat notification. Prior to the Government embarking on the proposed TSSR regime it would benefit all stakeholders to have visibility of the roles that each of the above are intended to play within the overall TSSR construct.

The Associations also have concerns with the absence of any guidance for providers on the sharing of information where a provider might operate on a multi-national basis and have a head office that is located offshore. Clarification is sought on what can and cannot be shared with head office under such circumstances.

Principle 4

Have measures to mitigate security risks reviewed independently.

Control: ITU-T Rec X.1051 – paragraph 6.1.8

The Associations support the proposal that a network infrastructure security regime should include a facility for an appropriate means of reviewing the measures for mitigating security risks, noting that it would need to be truly independent in terms of its ability to mediate in the event of a dispute. Reviews would be need to be conducted based on a set of pre-determined criteria that takes into account the risk level; whether the risk pertains to a high or low risk market segment; the likely benefits of the specific mitigation measures to affected services; and the potential cost to consumers of implementing the mitigation measure/s.

Should a review result in formal action being required, Industry seeks clarification of the means and timing for lodging an appeal against the action, i.e. can an appeal be lodged upon notification of a pending action, or after the action has been taken? The overall review process appears to lack specific parameters or criteria, with little justification for the need for periodical reviews and the frequency with which they are imposed.

Any review of mitigation measures should preclude the review of day-to-day operations. This would only increase administrative costs and would appear to undermine the Government's commitment to reducing red tape in the telecommunications sector.

Principle 5

Work with suppliers of equipment and services to identify and mitigate security risks across the telecommunications supply chain.

Control: ITU-T Rec X.1051 – paragraph 6.2.3

The Associations contend that where a provider's head office is based offshore and decisions on procurement are taken out of the hands of the Australian operations, compliance with an Australia-specific requirement to identify and mitigate security risks across the entire supply chain is problematic. Noting that procurement and supply is often conducted on a global basis, guidance from Government on suppliers or regions of concern would be beneficial for providers in terms of ensuring that procurements decisions can be taken with the proposed TSSR framework in mind.

In terms of ensuring that supply contracts include additional security mitigation measures, it is common practice that due diligence is already undertaken at the commencement, or during the renewal, of any commercial vendor agreement for the supply of infrastructure. The Associations are satisfied that this corporate due diligence should be sufficient. However, where the supply agreement relates to the reselling of services there is often a limit on the extent to which security mitigation measures can be applied and enforced.

Principle 6

Good physical security contributes to network resilience.

Control: ITU-T Rec X.1051 – paragraph 9

Ensuring that appropriate and effective physical security mitigation measures are in place is an accepted practice across Industry, noting that this practice exists without any existing regulations mandating as such. Measures are recorded and audited internally – the Associations feel that this documentation should provide sufficient comfort to the Government, noting however that some allowance should be made for remotely located network elements where physical logistics prevent the application of the same measures that might be in place for infrastructure that is based in, for example, a head office. Generally, risk mitigation strategies are in place for all critical network elements but this has not been acknowledged in Government's draft guidelines.

Further, the additional requirements being proposed would appear to contradict the Government's red tape reduction agenda, and also appear to overlook the fact that all providers have an ongoing commercial imperative to assess and mitigate any risks to network infrastructure.

Principle 7

Access to networks and facilities should be based on considerations of risks to data sovereignty and integrity.

Control: ITU-T Rec X.1051 – paragraphs 10.1.4, 10.2 and 11

The Associations seek clarification on the basis for this requirement as it is unclear at what point data sovereignty starts to become an issue for Government with respect to network infrastructure security, and why Government sees a need to involve Industry in such discussions when it would appear more a matter for inter-government relations. Even if clauses pertaining to sovereignty of information were to be inserted into commercial contracts it is not certain that anything could be done to enforce them where the laws of a foreign country might take precedence.

Principle 8

Proper incident management may avert a breach turning into a crisis.

Control: ITU-T Rec X.1051 – paragraph 13

The Associations acknowledge that incident management measures to address unforseen major network incidents (e.g. fibre cuts, natural disaster management) are critical, but note that such measures are already in place as part of standard telecommunications network incident mitigation processes, and as such regulation to mandate these measures is not required. All providers have a commercial imperative to protect their customers and corporate brand and accordingly Industry sees no justification for incident management specific regulation.

Principle 9

Factor the identification and treatment of security risks into system design and management accordingly.

Control: ITU-T Rec X.1051 – paragraph 13

Noting the importance of network security and resiliency in the digital age, the Associations on the whole supports the Government's security outcomes/objectives based approach as opposed to stipulating a requirement for Government approval of network architecture at a technical or engineering level, but points to the fact that processes for facilitating the identification of security risks into network and system design are already in place, thus

negating the need for specific regulation. Regardless, a greater degree of specificity in terms of recommended measures would be beneficial to providers. The Associations point to the detail contained in the OECD Guidelines for the Security of Information Systems and Networks1 , with its underlying mantra of promoting a 'culture of security' rather than a regulatory regime, as an example of the type of detail Industry would benefit from.

However, caution should be exercised when considering the implications of mandated objectives on the ability of providers to build a competitive advantage via network design and architecture.

4. Conclusion

The Associations look forward to continued engagement with Government on the proposed TSSR package and would welcome the opportunity to discuss, in greater detail, the feedback provided in this submission.

We also look forward to the publication of the Regulation Impact Statement that has been completed in respect of the TSSR proposal, as indicated in our most recent discussions.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au or Lisa Brown on 02 6239 6555 or at lisa.brown@amta.org.au.

[1] OECD Guidelines for the Security of Information Systems and Networks