COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Parliamentary Joint Committee on Intelligence and Security (PJCIS)

Review of Part 14 of the *Telecommunications Act 1997* – Telecommunications Sector Security Reforms (TSSR).

18 December 2020

Contents

1. Executive Summary

Communications Alliance welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of Part 14 of the *Telecommunications Act 1997* – Telecommunications Sector Security Reforms (TSSR).

Communications Alliance and its members were deeply involved in the development process of the TSSR. The implementation of the Reforms has had a significant commercial and operational impact on our members, who take their obligations to protect their networks, facilities and any associated infrastructure and their customers' data very seriously.

Our sector is subject to a number of security and resilience-related obligations under various pieces of legislation and (enforceable) co-regulatory instruments, many of which take an all-hazards approach. These existing layers of regulation ought to be taken into account when considering the interaction of the TSSR and the future Security of Critical Infrastructure (SoCI) regime.

The Positive Security Obligations (PSO) contained in the proposed revised *Security of Critical Infrastructure Act* (SoCI Act) to prepare and maintain a risk management program is intended to result in the same outcome as the TSSR. Imposition of the PSO on entities already subject to the TSSR's security and notification obligations will result in duplication of regulatory regimes that have the same intended outcome. We, therefore, recommend either repeal of the TSSR notification obligation or exemption from this obligation for entities subject to this PSO. If 'switched on' under the sector-specific rules of the SoCI Act, there is also potential for duplication of information gathering powers and directions powers which may drive up costs to consumers. Any duplication of regulatory regimes is likely to raise costs for service providers with potential consequential price increases for consumers.

With respect to the existing TSSR, we note that the current notification threshold and the risk assessment framework used for analysis of notified changes would benefit greatly from clarification. This could enable faster decision-making processes, decrease uncertainty, increase consistency and reduce costs for all parties involved.

It may also increase efficiency and reduce requests for further information if the Critical Infrastructure Centre explained what framework or standards it uses when undertaking its statutory role of assessing the proposed changes.

The two-way exchange of risk information, the resultant efficiencies and the flexibility of approach to deal with potential risks enshrined in the principles-based approach of the security obligation of Sections 313(1A) and (2A) of the *Telecommunications Act 1997* (Telco Act) form the building blocks of the TSSR.

Bilateral threat sharing – i.e. the promised proactive provision of threat information from Government to industry – has not occurred to the extent envisaged by our sector. Consequently, we recommend processes be implemented to improve and facilitate these data exchanges.

Our members value their relationship with the Critical Infrastructure Centre and the trust that has been built to informally exchange information under the TSSR framework. Steps to formalise some of these arrangements are, in our view, unwarranted. Equally, we do not believe that introducing additional prescriptiveness into the TSSR would be beneficial.

About Communications Alliance

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, see http://www.commsalliance.com.au.

2. Current security regulation and evolving landscape

The existing legislative framework for telecommunications contains – and the industry complies with – a number of obligations in relation to the security of the operators' networks and the communications that travel across those.

Part 14 of the Telco Act sets out the obligation to do the "carrier's best or the provider's best to protect telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access"[1] and to "give […] help as is reasonably necessary"[2] to officers and authorities of the Commonwealth and of the States and Territories (along with complementary immunity and 'no profit no loss' provisions) and includes the far-reaching TSSR protection, notification and approval requirements. We note that these obligations are not cyber security-specific, but go to broader obligations to protect networks or facilities from unauthorised access or interference. This has been interpreted, and applied, as requiring an 'all hazards' approach. For example, the revised TSSR Administrative Guidelines state that steps that a provider may do to demonstrate it is doing its best includes "considering risks to information security, and risks to physical security, personnel security and supply chain security."

Part 13 contains important non-disclosure requirements and also provides for the suspension of services in emergencies.

Part 16 of the Telco Act deals in part with responses to disasters and civil emergencies.

Part 6 of the Telco Act provides a framework for the development of enforceable industry Codes and Standards, including for the purpose of protecting end-users from scams as well as in relation to strategies to minimise the effect of compromised devices on end-users.

It is also worth highlighting that the telecommunications sector already has a framework of instruments and arrangements for an all-hazards approach to managing critical infrastructure impacts.

These include the:

- Emergency Call Service Requirements Code, dealing with protection of Triple Zero services, including in a cyber event (enforced by the ACMA);
- Triple Zero protocol that deals with all hazards that disrupt Triple Zero capability;
- Scam Reduction Industry Code that combats scam traffic impacts on networks and consumers;
- all-hazards Communications Protocol for managing telecommunications disruptions due to major emergency events;
- operation of the Communications Sector Group (a sub-group of the TISN), co-chaired by TPG Telecom; and
- the potential for disaster plans or network survivability plans under Part 16 of the Telco Act.

The sector is also focused on new arrangements for creating stronger communications infrastructure resilience capability – e.g. via additional back-up generators, cells-on-wheels (COWs) etc – in the wake of the 2019-20 bushfire events.

[1] Part 13, Section 313 (1A), *Telecommunications Act 1997*
[2] Part 13, Section 313 (3), *Telecommunications Act 1997*

Importantly, Government has recently concluded consultation on the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*. This draft legislation proposes to introduce further far-reaching security obligations that apply to a variety of critical infrastructure sectors and assets, including the telecommunications sector. The critical infrastructure assets captured under the current TSSR are also in scope of the proposed new SoCI Act.

On 10 December 2020, Government introduced the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (Bill) into Parliament with an intention of referring the Bill to the Committee in December and commencing the co-design of the sector-specific rules in January.

It is likely that the Committee will be asked to consider the revised SoCI Act in parallel to the ongoing review of the TSSR. This is also likely to be at the same time as the commencement of the sector-specific rules design. These multiple parallel processes make it difficult to provide a detailed contribution as the outcome of one process has implications for the others.

In the Explanatory Memorandum to the Bill, it is noted that the Government will consider the outcome of this review before turning the positive security obligations on for carriers and CSPs.

As the two frameworks both contain sets of requirements that seek to address similar or identical issues (i.e. ensuring the ongoing security and resilience of critical infrastructure assets, including through enhanced security in the supply chain and information sharing) it will be imperative to consider the TSSR alongside the proposed new legislation as well as other existing regulatory and legislative requirements for the our sector.

The review of the TSSR must have regard to the evolving horizontal regulations such as the SoCI Act and ensure that the rules of those regulations avoid overlap, redundancy or even inconsistencies with existing sector-specific regulations. Service providers which are already subject to cyber security requirements in sector-specific legislation must remain excluded from the scope of the horizontal requirements or see a removal of sector-specific regulation where those would create duplication. This exclusion is necessary to ensure legal clarity, certainty and proportionality of obligations.

We welcome the policy intent to work cooperatively and to avoid duplication: "Government will work in partnership with critical infrastructure entities to ensure the new requirements build on and do not duplicate existing regulatory frameworks. This approach recognises that many operators of critical infrastructure, particularly in the banking, finance, aviation, maritime and communications sectors already operate under regulatory frameworks that impose risk management, report and transparency obligations. Regulators in those sectors are already equipped to supervise those entities, identify emerging threats, and assist regulated entities respond to those threats. By focusing on outcomes, the new framework will ensure consistent security standards across all sectors without unnecessary regulator impost."[3]

3. TSSR and SoCI

As indicated throughout discussions with the Department of Home Affairs and as set out in SoCI Bill, the TSSR requirements largely apply to the same entities and infrastructure assets as envisaged to be in scope for the PSO and/or Systems of National Significance (SoNS) of the Bill

As one element of the PSO (which are to be 'switched on' for respective critical infrastructure assets), the Bill proposes that the owners of such critical infrastructure assets

[3] p. 12, Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance*, Consultation Paper, August 2020

prepare, comply with and maintain an all-hazards risk management program, which is to be endorsed by the Board of the entity and reported to the regulator.

We argue that, in effect, this makes the TSSR notification requirements redundant as assessment of the risks of proposed changes would necessarily form part of a broader, annually endorsed and reported risk management plan.

Subjecting entities to the TSSR notification requirements (and subsequent risk mitigation if deemed necessary) as well as the PSO of the revised SoCI Act would result in a substantial amount of duplication and inefficiencies – the opposite of Government's stated aim. Consequently, only one of the two requirements ought to apply to critical infrastructure entities in the telecommunications sector. We suspect that maintaining both sets of obligations would equally create duplicative efforts for the CAC/Critical Infrastructure Centre.

To avoid such duplication, we recommend implementing one of two options:

1. Repeal of the TSSR notification requirements of Part 14 of the Telco Act in parallel with the enactment of the Bill.
2. Exemption of telecommunications entities that are subject to the PSO requiring a risk management program or that operate a SoNS (within the meaning of the revised SoCI Act) from the TSSR notification obligations. This could be achieved with relatively little administratively effort by stipulating in the revised SoCI Act that a Ministerial declaration to subject an entity's asset to the PSO act as a trigger for consideration by the CAC to grant an exemption from the respective TSSR requirements. Section 314A(5A) of the Telco Act already provides the CAC with the own-motion power to make such decisions.

Information gathering and directions powers should also not be duplicated. This could be achieved by not 'switching on' these powers in the sector-specific rules envisaged by the proposed SoCI Act as telecommunications entities are already subject to similar powers under the TSSR.

We believe that there should only be one authority designated for CSPs in the security space. Currently, the legislative and regulatory environment around security, cyber security and data protection is rather crowded. This may also lead to duplication or overlap in requirements in some areas. We welcome the PJCIS' efforts in facilitating a coordinated and streamlined approach to security requirements for telecommunications and digital services, and encourage all relevant regulators to work together to minimise regulatory burden.

4. Notification threshold, assessment criteria and timing

Section 314A of the Telco Act requires nominated carriage services providers (NCSPs) to notify the Communications Access Co-ordinator (CAC) if a proposed change to a NCSP's network or facilities "is likely to have a material adverse effect on the capacity of the carrier or provider to comply" with the security obligations of Section 313(1A) and (2A).

However, it has proven difficult for NCSPs to determine the threshold as to when a proposed change would have a material adverse effect in this context. For example:

- Is this the effect from the proposed action that would result if no risk mitigation measures were to be applied? or
- Is the threshold of having a material adverse effect only met when a proposed action would result in a residual risk of such an effect after risk mitigation strategies have been applied?

Depending on how this threshold question is being interpreted, NCSPs may take different approaches to notification of proposed changes.

Similarly, and related to the above, it is unclear to NCSPs which precise criteria, risk assessment framework and/or security standards the CAC applies when assessing a notified change (or when considering a proposed change discussed informally with an NCSP).

A clear understanding of the notification threshold and the assessment criteria would greatly assist our members in making consistent decisions (within their organisations and across the sector) with respect to notifications and allow them to submit notifications against the background of the risk assessment framework used by the CAC. This, in turn, is likely to reduce the need for clarification, enable faster decision-making processes and, ultimately, reduce costs for Government, NCSPs and consumers.

The TSSR legislation is silent on the timing of notifications. NCSPs appear to have the choice to either:

- Notify early on in a project when the NCSP may only have formed a preliminary view as to whether the notification threshold of a material adverse effect may be reached by a proposed change (noting the difficulty of determining such threshold). At this stage in the project, many variables may not be known or be conclusively determined. This may complicate notification and an exact description of the proposed change and its potential effect and, consequently, may make a reliable review by the CAC difficult. On the other hand, early input from the CAC may be helpful for the NCSP in forming opinions about risks, taking investment decisions or finalising contracts. Nevertheless, even with an early involvement of the CAC, two or more notifications for the same proposed change may be required; or
- Notify at a significantly later stage in the project when most variables are known and many decisions have been taken, or at least have progressed significantly. Later notification provides the advantage of the NCSP having gained a better understanding of the proposed change and whether the notification threshold will be reached and, if so, of being able to supply significantly more detail to the CAC as part of the notification process, thereby allowing for a more informed and faster review process. However, this approach bears the risk of the CAC potentially requiring a (significant) change to the project path (e.g. vendor selection) with attendant inefficiencies and costs.

It appears that both approaches may have merit and are being considered by NCSPs depending on their respective risk profiles, the proposed change and its operational circumstances. Consequently, we are not advocating for a legislated timing for notification.

However, the difficulties associated with either approach highlight the importance of proving clearer guidance around the notification threshold and the risk assessment framework so that the number of 'unknowns' and factors contributing to the risk that is inherent in any commercial project can be minimised.

5. Two-way threat sharing

Communications Alliance and its members have been involved in the development of the TSSR from its inception in 2014. Throughout the process, improved two-way risk sharing, including for the purpose of assisting CSPs with compliance with the security obligation, was a focal point of discussion and promised outcome of the Reforms once implemented.

Unfortunately, with the exception the Government 5G Guidance provided to a small number of CSPs in 2018, communications-specific threat information has not been shared with our members. Consequently, our members have borne substantial costs to implement the Reforms – and Government decisions that were taken as a result of the Reforms – without having had the promised benefit of additional risk and threat information to guide investment decisions.

This is regrettable and ought to be remedied with urgency, particularly in light of the additional layer of security regulation that the revised SoCI Act (even in its 'lightest version') is likely to represent for our sector.

6. Costs

More so than most other industries, the telecommunications industry acts as an enabler for the functioning of our modern economy. Our sector has already incurred substantial costs in the course of the implementation of the TSSR and continues to bear high regulatory expenses for ongoing compliance with various security-related legislative/regulatory requirements.

Against this background and noting the additional costs that are likely to result from the requirements of the revised SoCI Act, we encourage the Committee to consider cost recovery options for telecommunications providers covered under these extensive security regimes.

We deem it important that the critical infrastructure reforms and the TSSR preserve the principle of cost recovery, which is well established under the Telco Act, for example where C/CSPs provide assistance under section 313 of that Act.

7. Conclusion

Communications Alliance looks forward to continued engagement with the Committee, the Department of Home Affairs and other relevant stakeholders on the review of the TSSR and the revised SoCI Act – these two processes and the content of the two pieces of (draft) legislation are necessarily intertwined.

To the largest extent possible and only to the extent required, Australia's national security framework ought to build on and enhance existing legislative frameworks and industry efforts without introducing duplicative obligations. A thorough and evidence-based analysis is required to ensure current reforms are not duplicative or, worse, contradictory.

We share Government's desire to create a robust, effective and efficient framework that appropriately protects Australia's critical infrastructure and supply chains and stand ready to work with all stakeholders to create such a framework.

We support the adoption of a high-level principles-based approach to ensuring security. Such an approach allows CSPs the necessary flexibility to implement measures as appropriate for their business while being able to rapidly adapt to technological change. This approach is also more likely to avoid duplication or inconsistencies with existing (or future) international standards and best practice, and provides the necessary flexibility for globally operating organisations to comply with a more limited set of security specifications, thereby contributing to increased operational efficiency and legal certainty.

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

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