COMMUNICATIONS ALLIANCE LTD

Communications Alliance Submission

to the Department of Infrastructure, Transport, Regional Development and Communications

in response to the Exposure Drafts of the

Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022

and the

Telecommunications (Carriage Service Provider – Security Information) Determination 2022

29 March 2022

CONTENTS

Communications Alliance

Communications Alliance is the primary communications 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, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

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

1. Introduction

Communications Alliance welcomes the opportunity to make a submission to the Department of Infrastructure, Transport, Regional Development and Communications (Department) in response to the Exposure Drafts of the *Telecommunications (Carrier Licence Conditions – Security Information) Declaration 2022* (Licence Conditions) and the *Telecommunications (Carriage Service Provider – Security Information) Determination 2022* (CSPD).

We continue to support Government's Critical Infrastructure Reforms and welcome any steps to foster sustained practical industry-Government engagement and bilateral information sharing arrangements.

2. Duplicative regulatory regimes

2.1. We support the general policy objective underlying the Critical Infrastructure Reforms for protecting the essential services Australians rely on, by improving the security and resilience of critical infrastructure, including in the telecommunications sector.

2.2. We consider that amendments to the *Telecommunications Act 1997* (Act) as a way of avoiding regulatory duplication and providing clarity for the telecommunications sector is an appropriate way of undertaking this significant reform.

2.3. However, we do not support the use of Licence Conditions or a CSPD as the sole means to translate the Positive Security Obligations (PSO) of the Critical Infrastructure Reforms into rules for our sector, while simultaneously seeking to avoid duplication with existing legislation and regulation in the telecommunications sector.

2.4. Therefore, we strongly support the Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommendations to establish a telecommunications working group, comprised of government and industry stakeholders. As intended by the Committee, this working group can then "*be tasked with scoping agreed carrier licence conditions, service provider rules, and codes and standards for security of networks and systems. These can then be used to guide the resources to be produced by that group and inform directions or information gathering powers exercisable by the Minister for Home Affairs under the existing provisions of Part 14 of the Telecommunications Act 1997.*"[1]

2.5. Importantly, this working group ought also to be used, as recommended by the PJCIS, to "*be consulted to reach an agreed position regarding any duplicated security obligations that may be activated under an amended Security of Critical Infrastructure Act 2018 before they are activated. If agreed, and once activated, the duplicated obligations or other mechanisms in Part 14 of the Telecommunications Act 1997 should be repealed, or deactivated by relevant mechanisms, so as to avoid regulatory duplication on telecommunications entities.*"[2]

2.6. In the absence of the implementation of the two recommendations, presumably due to lack of time at this current stage, the proposed Licence Conditions and CSPD ought to be amended to include a sunset period of twelve months.

2.7. Against the above background, we note that the current telecommunications legislative and regulatory framework, acts to create a robust and operationally reasonable security regime for critical telecommunications infrastructure.

2.8. While some of the requirements described in the draft instruments may not be present in exactly the same form in the TSSR or elsewhere in the regulatory framework, elements that target the same outcomes are already existent under the current regime and

[1] pp.47/48, para 3.119, Rec. 4, Parliamentary Joint Committee on Intelligence and Security, *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms,* Feb 2022
[2] p, 50, para 3.134, Rec. 6, Parliamentary Joint Committee on Intelligence and Security, *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms,* Feb 2022

regulatory duplication will likely be unavoidable if no further consolidation of obligations is effected.

2.9. Consequently, we recommend a holistic and thorough analysis of the legislative and regulatory security framework, with a view to eliminating (repealing) areas of duplication that would otherwise occur in other legislation.

3. Carrier/CSP Asset definition

3.1. The draft Licence Conditions and the CSPD define 'asset of a carrier'/'asset of an eligible carriage service provider' (in the following 'C/CSP asset' for ease of writing) to include

> "*(i) a component of a telecommunications network*
>
> *(ii) a telecommunications network*
>
> *(iii) a facility*
>
> *(iv) computers*
>
> *(v) computer devices*
>
> *(vi) computer programs*
>
> *(vii) computer data"*

Especially, the inclusion of broad terms such as 'components' and 'computers' widens the scope of the definition so that almost anything within a carrier/CSP network appears to be included in the asset definition.

In our view, the definition is unworkable in its practical application, as all relevant requirements of the draft Licence Conditions and the CSPD reference the asset definition. We also question the usefulness of the definition for the Secretary of Home Affairs, as the amount of information received as a result of this overly broad definition is likely to be vast and unhelpful in the pursuit of the objective.

3.2. No evidence has been provided as to why a different approach has been chosen to that already in place under the *Security of Critical Infrastructure Act 2018* (SoCI Act): the equivalent requirements to register assets (Part 2, SoCI Act) and to notify cyber security incidents (Part 2B, SoCI Act) both pertain to 'critical infrastructure assets', i.e. transposed into the telecommunications sector, this would mean that the requirements would, if being dealt with under the SoCI Act, apply to 'critical telecommunications assets'.

Applying the obligations to 'critical telecommunications assets' instead of the definition of 'carrier/CSP asset' would not only be consistent with the approach taken in the SoCI Act (and make consistent use of the definition) but also makes practical sense, given that the proclaimed aim is to have an understanding (and possible opportunity for intervention) of ownership and locality of critical infrastructure in Australia, and obtain notification of (and opportunity for intervention, learning, threat sharing etc.) cyber security incidents with respect to infrastructure where those incidents are likely to significantly affect our society.

3.3. An overly broad asset definition risks 'drowning out' critical information and notifications on both accounts. The breadth of the definition also appears to create unnecessary regulatory burden with respect to the large amount of operational information that would need to be provided. (Also refer to our comments in Section 5 below.)

3.4. Consequently, we request that the asset definition proposed in the Exposure Drafts be replaced with the definition of 'critical telecommunications asset' as currently included

in the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (SLACIP Bill) as passed by the House of Representatives on 16 February 2022.

> ***"critical telecommunications asset** means:*
>
> *(a) a telecommunications network that is:*
>
> *(i) owned or operated by a carrier or a carriage service provider; and*
>
> *(ii) used to supply a carriage service; or*
>
> *(b) a facility (within the meaning of the Telecommunications Act 1997) that is:*
>
> *(i) owned or operated by a carrier or a carriage service provider; and*
>
> *(ii) used to supply a carriage service.*
>
> *Note: The rules may prescribe that a specified critical telecommunications asset is not a critical infrastructure asset (see section 9)."*

3.5. Importantly, we also note that the SoCI Act provides a mechanism for exemption of assets. This exemption mechanism is absent from the Exposure Drafts of the Licence Conditions and the CSPD and ought to be included.

3.6. Even if the 'critical telecommunications asset' definition outlined above is used, our members are very concerned about the significant regulatory burden that will flow from the requirement to provide operational information about their critical assets, given the very broad nature of this definition; capturing items such as pits and poles.

3.7. In this context, from a practical perspective, the instruments should allow for a materiality threshold to be applied to the assets which are required to be reported to the register. The register is designed to improve knowledge, so that Government can proactively assess national security risks related to an asset that is critical to national security. It is, in our view, not necessary or proportionate for the register to include operational information about each pit, for example.

4. Notifications of cyber security incidents

Notifications

4.1. As indicated above, the redefinition of assets captured in the draft Licence Conditions and the CSPD will not only be important for C/CSPs from a compliance perspective, but will be equally important for Government to ensure it is receiving information about critical and other cyber security incidents that have affected assets of sufficient criticality to warrant notification.

4.2. Section 10(2) of both draft instruments requires C/CSPs to notify critical cyber security incidents when those have *"a significant impact (whether direct or indirect) on the availability of an asset if, an only if, both: the asset is used in connection with the provision of essential goods or services; and the incident as materially disrupted the availability of those essential goods or services."*

4.3. However, neither the draft instruments (and also not the SoCI Act nor the SLACIP Bill) define essential goods or services. Consequently, it would be useful, it the instruments contained a definition for that purpose, to ensure that C/CSPs only notify critical incidents and do so to a uniform threshold.

4.4. On a related matter, we point out that carriage service intermediaries may not know what kind of applications their customers may be using their services for. Accordingly, these providers may be unable to determine whether a cyber security incident has reached a certain criticality threshold. It would be useful to understand where reporting obligations lie in such a scenario.

4.5. We are also concerned that the threshold for reporting 'other cyber security incidents' needs to be revisited to provide clearer criteria and avoid the unnecessary burden and distraction of reporting of low-level incidents.

4.6. While the proposed Licence Conditions and the CSPD include relevant threshold tests, we see the risk that the current definition, in combination with a tendency to err on the side of caution, may lead to a potentially very large number of notifications, which may 'drown out' the actually relevant notifications.

4.7. In our view – and from conversations with the Department of Home Affairs – it was our understanding that this was the stated aim, i.e. that our sector ought to be formalising the voluntary threat and incident reporting arrangements that are already occurring for substantial parts of our sector. Such reporting ought to occur on the basis of a C/CSP-specific materiality threshold.

4.8. We recommend discussions with our sector whether the threshold for reporting of 'other cyber security incidents ought to be set in line with the C2 level incident of the 2020 ACSC Incident Categorisation Matrix.

Protection from Liability

4.9. Section 30BE of Part 2B of the SoCI Act exempts an entity from liability for an action or other proceeding for damages in relation to an act done or omitted in good faith in compliance with the respective cyber security incident reporting obligations of that Act. Similarly, officers, employees or agents of an entity are equally not liable for acts done or omitted in good faith in connection with those obligations.

4.10. These protections are missing from the proposed Carrier Licence Conditions and the CSPD and ought to be inserted to protect C/CSPs.

5. Operational information

5.1. C/CSPs are required to report operational information as set out in section 6 of the draft Carrier Licence Conditions. Section 6(1)(d) includes *"a description of the arrangements under which the carrier operates the asset or part of the asset"*. To provide clarity for C/CSPs the instruments should provide examples of what type of information is sought when asking for *"a description of the arrangements"*.

5.2. Such operational information also includes *"a description of the arrangements for the maintained data"* (Section 6 in both draft instruments). C/CSPs are very concerned about the regulatory burden in providing such information and urge the Department to further consider whether the benefits of providing this information outweigh the attendant cost.

5.3. 'Maintained data' is defined as

> ***maintained data*** *is data that:*
>
> *(a) relates to an asset of an eligible carriage service provider; and*
>
> *(b) is maintained by an entity other than the eligible carriage service provider; and*
>
> *(c) is any of the following kinds:*
>
> *(i) personal information (within the meaning of the Privacy Act 1988) of at least 20,000 individuals;*
>
> *(ii) sensitive information (within the meaning of the Privacy Act 1988) that relates to any individual;*
>
> *(iii) information about any research and development related to the asset;*

(iv) information about any systems needed to operate the asset;

(v) information about risk management and business continuity (however described) for the asset;

(vi) information about consumers' consumption of listed carriage services or any directly-related product.

5.4. This definition is, again, very broad and includes information of a public nature (e.g. it could include any manual or any publicly available research), just because that information may relate to an asset under consideration.

5.5. Consequently, items (iii) to ((v) ought to be re-drafted to reflect that only information that is not public and absolutely critical to the operation of the asset and/or risk management/business continuity of the asset is included in the definition. Otherwise, the reporting obligations for operational information would become completely impractical (noting the already broad definition of the underlying asset, independent of the asset definition that will be adopted).

5.6. The 'description of the arrangements for maintained data' must include, amongst other things, "*the physical address where the data is held, including, to the extent practicable, the physical address where computers or servers holding the data are located, whether or not the computers or servers are part of a cloud service or software-as-a-service*" (Section 6(2)(d) of both instruments).

5.7. We submit that there should be an exemption for C/CSP groups, i.e. the maintained data reporting should not be required if the entity that maintains the data is a related body cooperate.

5.8. Importantly, we note that the proposed requirements could amount to a security risk and/or administrative challenge to map the physical address of computers and services holding data considering the range of data captured and the complexity of the systems involved. In some cases, obtaining this information from suppliers would already be a substantial challenge.

5.9. Consequently, this requirement ought to be removed.

5.10. However, given the number of issues arising from the definition of 'maintained data' and 'operational information', we urge the Department to reconsider these definitions and the obligations tied to it and to craft a more narrowly focused framework that targets critical assets, data and operational information in line with the desired objectives of understanding the location and ownership structures and ensuring the security of truly critical infrastructure.

6. Group asset registers

6.1. Many C/CSPs operate in entity groups, i.e. they hold several carrier licences and may also control several CSPs. They may choose to market their products and services under one corporate brand, or distinct brands.

We believe it would be more practical for C/CSPs and the receiving end (Secretary of Home Affairs) to make provision in the draft instruments for group asset registers, i.e. to allow C/CSPs to maintain and report on the relevant operational and interest and control information of direct interest holders in relation to the relevant assets at a group level, that is not submit multiple reports for each carrier or eligible CSP that may be within the group.

7. Ransomware attacks

7.1. Section 10 of the draft Licence Conditions and the CSPD both require notification of a 'critical cyber security incident' where the incident *"has had, or is having, a significant impact (whether direct or indirect) on the availability of any of its assets"*.

7.2. Noting that Section 11 of both draft instruments sets a wider threshold for 'other cyber security incidents', we seek clarification as to whether Section 10 (Notification of critical cyber security incidents) is intended to allow the exclusion of ransomware attacks where those do not meet the threshold of significantly impacting on the availability of the provider's asset (which may be the case).

8. Implementation period

8.1. Section 12 of the draft Licence Conditions and the CSPD provides for a six months' grace period with respect to the operational information that must be provided in relation to each asset and in relation to the interest and control information of direct interest holders in the asset.

8.2. However, the draft instruments do not propose a similar or even three months' grace period for the cyber security incident notification obligations.

8.3. We note that the draft *Security of Critical Infrastructure (Application) Rules 2021* (Rules) include a three months' grace period for these obligations.

8.4. While we recognise that the Rules would not apply to our sector, we believe that our sector ought to equally benefit from a three months' grace period in order to be able to implement the required processes and systems for incident notification on a wide range of 'critical telecommunications assets' (preferably under this definition).

9. Statutory review

9.1. The proposed rules are a significant additional regulatory impost on our sector. It is, therefore, key to ensure that the regime functions as intended, with minimal costs and without unintended consequences (as, for examples, was the case with the Data Retention Regime, and also, in part, with the Telecommunications Sector Security Reforms (TSSR)).

9.2. As commented above, we believe the Licence Conditions and CSPD ought to be subject to a twelve months' sunset period.

9.3. If the two instruments were to be remade after that period – after deliberations with all stakeholders within the working group established as recommended by the PJCIS – we believe the instruments ought to include a mandatory statutory review two years after their renewed commencement.

10. Conclusion

Communications Alliance looks forward to continued engagement with the Department and all relevant Stakeholders on the development of practical and non-duplicative rules that focus on the key outcomes of notification and information provision for truly critical assets for the telecommunications sector. We remain committed to shared objective to protect our critical infrastructure from interference and make it resilient in times of emergencies.

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