COMMUNICATIONS
ALLIANCE LTD

Communications Alliance submission

to the

Department of Home Affairs Critical Infrastructure Centre

Draft Critical Infrastructure Asset Definition Rules

14 May 2021

Contents

1. Introduction

Communications Alliance welcomes the opportunity to provide a submission to the Department of Home Affairs Critical Infrastructure Centre consultation on the Policy Paper Protecting Critical Infrastructure and Systems of National Significance, Draft Critical Infrastructure Asset Definition Rules.

This submission builds in part on the feedback previously provided to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) reviews of the *Security Legislation Amendment (Critical Infrastructure) Bill* 2020 (Bill) and Statutory Review of the *Security of Critical Infrastructure Act* 2018 and the Statutory Review of Part 14 of the *Telecommunications Act 1997* – Telecommunications Sector Security Reforms (TSSR).

2. Process

2.1. From the material provided (Policy Paper Protecting Critical Infrastructure and Systems of National Significance, Draft Critical Infrastructure Asset Definition Rules, April 2021), we understand that 12 of the of the identified 22 asset classes require further rules to be made to finalise the asset-sets subject to the expanded regulatory framework.

2.2. We also note that the Policy Paper states that another 10 critical infrastructure asset classes do not require threshold definition rules and "do not require further rules as they have been fully defined in the Bill"[1](emphasis added). Critical telecommunications assets and the critical data storage and processing assets are both deemed to fall into this category.

2.3. It appears that the focus of the consultation, or indeed the sole purpose of the consultation, is to seek feedback on the 12 asset classes that require additional rules to be made and which are the subject of pp. 1-30 of the Policy Paper.

2.4. However, it is not clear to us whether there is an intention to consult with those sectors whose critical infrastructure assets do not require (but allow for) further rules to be made and, if so, at what stage this would occur.

2.5. We are concerned by the implied assertion that the critical infrastructure assets of the data storage and processing sector and the telecommunications sector have been defined comprehensively, or indeed in an operationally workable manner, in the Bill.

2.6. For the reasons outlined below, we strongly recommend that Government make use of the powers allowed for under section 9(2) that would allow for rule-making to prescribe that certain specified critical telecommunications and data storage and processing assets (i.e. those that would ordinarily be captured by the broad definitions of the Bill) are not critical infrastructure assets.

2.7. Consequently, we recommend that, either now or, at latest during the co-design phase of the rules for the respective sectors, the definition of critical infrastructure asset should be subject to further consultation with a view to practical threshold tests. We make some proposals in this regard in Section 3 below.

2.8. We also urge Government to provide clear guidance on implementation timeframes, and indeed to set reasonable and realistic (phased) implementation timeframes for the respective sectors.

3. Critical Telecommunications Asset

3.1. The definition of 'asset' is very broad – in fact the 'definition' is a non-exhaustive list of items that may be considered an asset, rather than a clear definition of the term.

3.2. Importantly, the term 'critical telecommunications asset' is almost as broad in that the only criteria of such a classification are:

- Owned or operated by a carrier and use to supply a carriage service; or
- Owned or operated by a carriage service providers (CSP) and or use [of the asset] in connection with the supply of a carriage service'.

3.3. While we agree that it is indeed the use (or function within the network, see para. 3.15/3.16 further below) that is likely to determine the criticality of an asset, the inclusion of all assets used to supply any carriage service is too wide. This definition will include assets forming part of small networks that are not critical infrastructure; many networks provided where there is a fully substitutable alternative (making availability not critical)

[1] p. 30, Department of Home Affairs, Protecting Critical Infrastructure and Systems of National Significance, Draft Critical Infrastructure Asset Definition Rules, April 2021

and many IoT and machine-to-machine communications that carry data that is not critical to national security.

3.4. The definition of CSP in section 87 of the *Telecommunications Act 1997*does not exclude but rather encompasses carriers. Accordingly, the term CSP covers the telecommunications sector. This means that the distinction between carriers and CSPs drawn in paragraph (a) and (b) of the definition of critical telecommunications asset is redundant. If the intention is for paragraph (b) to apply only to CSP that are not carriers, the definition should be amended accordingly.

3.5. The requirement that the asset of a CSP be treated as critical infrastructure for mere 'use in connection with the supply of a carriage service' arguably casts the net so wide that almost every asset in the telecommunications sector is, by definition, a critical telecommunications asset.

3.6. The consequences of this far-reaching definition are not trivial – in effect they make it almost impossible to meaningfully operationalise the positive security obligations, particularly around the risk management program.

3.7. If almost any asset – including payroll systems, ordering platforms, contractor management systems, complaint logging and management systems etc. – is considered a critical telecommunications asset, because it is used 'in connection with the supply of a carriage service', then, following the requirements of section 30AH, C/CSPs would need to (and noting the various 'on-switches' that may trigger different obligations, it would appear that <u>all</u> telecommunications C/CSPs are captured by the legislation):

- catalogue each asset – a major undertaking in and of itself;
- "identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset";
- so far as reasonably possible, "minimise or eliminate any material risk of such a hazard occurring"; and
- "mitigate the relevant impact of such a hazard on the asset" (and comply with any other rules, if any).

3.8. The objectives of the legislation can be achieved without the sweeping imposition of red tape proposed. We suggest that IoT networks be exempted (noting that any network that develops or is used for a purpose critical to national security might be included by specific nomination). We suggest, consistent with the policy for electricity, gas, water and sewerage, that all telecommunications networks that service less than 100,000 services in operation be exempted.

3.9. We also note that section 5(bc) now extends the definition of 'protected information' to include all information that "is, or is included in, a critical infrastructure risk management program that is adopted by an entity in compliance with section 30AC". It, therefore, also includes all information on assets listed as part of the risk management program.

3.10. Section 41 in turn limits disclosure of such information by the entity, i.e. the C/CSP, to instances where the disclosure occurs as part of exercising duties or functions under or to comply with the Act (*Security of Critical Infrastructure Act 2018*). It is, in our view, almost impossible to conduct any normal business operations without disclosing asset information – noting the almost all-encompassing definition of 'critical telecommunications asset' above – without running the risk of breaching the non-disclosure obligations of Section 41.

3.11. Consequently, it is imperative that the definition of 'critical telecommunications asset' be further clarified and limited, in order to shape a definition that is practicable while still achieving the desired security outcomes.

3.12. It is our understanding that, with respect to the assets covered, the policy intent of the critical infrastructure reforms for our sector was to mirror those assets that are captured by requirements of the TSSR.

3.13. The security obligation introduced into section 313(1A) of the *Telecommunications Act 1997* by the TSSR requires C/CSPs to their best to protect networks and facilities from unauthorised access and interference to ensure "the confidentiality of communications carried on, and of information contained on, telecommunications networks or facilities; and the availability and integrity of telecommunications networks and facilities".[2]

3.14. In essence this means that the TSSR security obligation requires the protection of its critical assets in order for a C/CSP to be able to discharge of its TSSR obligations.

3.15. The *Telecommunications Sector Security Reforms Administrative Guidelines* further highlight that the "following parts of networks and facilities are generally considered to be most sensitive. 'Sensitivity' is established based upon the following three impacts:

- availability impact: the damage to the network of the equipment going offline
- integrity impact: the disruption caused by changing the data over which the equipment has control
- confidentiality impact: the cost of compromise of data within the network equipment." [3]

The Administrative Guidelines go on to list four key areas that appear to generally fall into this category of 'core and sensitive network facilities'. Those are:

- Network Operations Centres;
- Lawful interception equipment or operations;
- Parts of networks that manage or store an aggregate of information; and
- Locations where traffic belonging to customers or end users is aggregated in large volumes, either in transit or at rest.

(The Administrative Guidelines provide further detail on each of those points.)

3.16. Analogously to the TSSR[4], we propose that the definition of the asset ought not to hinge only on whether it is used in connection with a carriage service but rather on whether interference with the asset would have a relevant impact on the desired security outcome for the network of facility, i.e. the sustained availability, reliability and integrity of the network or facility and/or confidentiality of communications/information.

3.17. The Administrative Guidelines for the TSSR assist with the assessment of assets, in that they indicate which assets and facilities are likely to fall into this category. The same guidance ought to apply for C/CSPs in their deliberations when they develop and comply with their positive security obligations, including their risk management programs.

3.18. We also note that, in many cases, telecommunications services are not provided and networks and systems (and underlying assets) are not owned by a single C/CSP but rather by multiple entities that act as one corporate group, which may have include a number of C/CSPs. Even individual assets may be co-owned by C/CSPs within a C/CSP group and, of course, across shareholders and investors. Additionally, the telecommunications services, networks and systems belonging to one C/CSP or C/SCP

[2] Section 313(1A)(c) and (d), *Telecommunications Act 1997*
[3] p. 15, Australian Government, Critical Infrastructure Centre, Telecommunications Sector Security Reforms Administrative Guidelines, October 2018
[4] Communications Alliance has proposed legislative options to reduce the inherent overlap of the security of infrastructure reforms with the existing TSSR; please refer to Section 3 of our submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the statutory review of the TSSR.

group may be utilised by a third-party C/CSP to provide services. This complexity needs to be addressed to make the proposed obligations workable.

3.19. For example, the four largest internet service provider groups (ISP groups) in Australia consist of around 46 individual entities. This further complicates the picture. We seek clarification whether C/CSPs would be permitted to adopt, maintain and report on one critical risk management program (and other material required under the Bill) on a group level.

4. Critical Data Storage and Processing Asset

4.1. We welcome the omission of the reference to commercial services in the definition of 'data storage or processing sector' in the Bill as introduced into Parliament in December 2020, thereby broadening the definition to a more appropriate neutral scope that includes all services, regardless of whether they are offered on a commercial or non-commercial basis.

4.2. However, the amendment of the sector definition will not be helpful unless also the definition of 'critical data storage or processing assets' in section 12F is equally amended to omit all references to commercial services. We submit that all services ought to be secured to the same high level independent of whether a critical infrastructure entity manages, processes, stores etc. data in the public cloud, 'on-site', with a third party or through some other model. The Bill ought to be amended to reflect these considerations.

4.3. Moreover, the definition of 'critical data storage and processing asset' contained in section 12F appears to be flawed or misleading in that on one reading it seems to measure the criticality of the asset by whether the asset "is used wholly or primarily to provide a data storage or processing service that is provided by the entity […] to an end-user", instead of asking the question whether the data stored or processed (and therefore potentially put at risk) is critical for the running of critical infrastructure.

4.4. To illustrate the matter, consider the following examples:

- Data storage and processing entity A owns a very small server and stores 0.05% of the data of a very large bank. The bank's data consume 90% of entity A's server capacity. Entity A's storage and processing service 'relates to' business critical data' and entity A is aware of this. (Note that the broad language 'relates to business critical data' may be another issue that requires clarification.) Therefore, entity A's server is a critical data storage and processing asset, and entity A is the responsible entity.
- Data storage and processing entity B owns a very large server and stores 90% of the data of a very large bank. The bank's data consume 20% of entity B's server capacity. Entity B's storage and processing service 'relates to' business critical data' and entity B is aware of this. In this scenario, despite the criticality of the data, entity B's server is NOT a critical data storage and processing asset as the condition of section 12F(b) "wholly or primarily used to provide a data storage or processing service that is provided by the entity […] to and end-user" has not been satisfied. Entity B is NOT a responsible entity (at least not in relation to this asset).

4.5. We note also that identification of data storage and processing services by who they serve is duplicative of existing regulation:

- Critical Infrastructure assets are required to report operational information including "a description of the arrangements under which data prescribed by the rules relating to the asset is maintained" (section 7(f) of the Security of Critical Infrastructure Act 2018). This reporting obligation and the powers available to the Minister if not satisfied with the national security implications of the information

provided, already operate to ensure the security of data storage and processing by responsible entities.

- The finance sector is subject to statutory obligations (*Corporations Act 2001* sections 912A(1)(a), (b), (c), (d) and (h) and (5A)) and CPS 234. In particular, CPS 234 will apply to almost every responsible entity in the finance sector and includes a range of data security requirements that require control and management of outsources services, including para. 16, which provides "Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets."

4.6. These examples highlight that the 'critical data storage and processing asset' definition ought to be re-considered/clarified, to ensure it achieves the desired objective, i.e. the protection of business-critical data where this data is relevant for the operation of a critical infrastructure asset. In aiming for this objective, it is important to keep in mind the primary responsibility of the critical infrastructure asset to ensure that outsourced services are secure and reliable. Also, that it is standard practice in the industry to maintain redundancy and back-up systems for critical data.

4.7. We understand that on another reading the term 'wholly or primarily used to provide a data storage or processing service' may be understood to mean that the entity wholly or primarily provides that service (data storage and processing) as opposed to some other ancillary service such as accounting. However, given to criticality of the definition, we believe the definition ought to be clarified as per our suggestion above and its meaning put beyond any doubt.

4.8. We also seek guidance on a more legal aspect: it appears that the language used in the definition of section 12F of "a body corporate established by a law of a Territory" would exclude local councils in NSW which are "body politics" under the *NSW Local Government Act 1993* although they are "to be treated by the law of the state in the same way as it applies to and in respect of a body corporate" (section 220 of that Act) Does the same apply in all other States and Territories?

5. Space Technology Sector

5.1. Section 8D of the Bill list the space technology sector as critical infrastructure sector.

5.2. The sector is – very broadly – defined in section 5 of the Bill as "the sector of the Australian economy that involves the commercial provision of space-related services". The note accompanying the definition list includes a non-exhaustive list of examples of space-related services, such as:

- position, navigation and timing services in relation to space objects;
- space situational awareness services;
- space weather monitoring and forecasting;
- communications, tracking, telemetry and control in relation to space objects;
- remote sensing earth observations from space;
- facilitating access to space.

5.3. The Explanatory Memorandum to the Bill notes that the "definition is intended to capture the assets that provide the services, as well as those that support them."[5]

5.4. The Bill does not contain a definition of 'critical space technology asset'. Importantly, the Policy Paper also does not contain any proposed rules or definition of the term.

[5] para. 246, *Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020*

5.5. Therefore, we seek clear and early guidance on what assets would be considered critical in this respect. For example, would a C/CSP that provides communications services to a weather monitoring and forecasting services organisation be also captured within the space technology sector? Or would the link have to be closer, such as actually owning/operating the satellites used for such services?

5.6. We also seek guidance on how duplication and complexity will be reduced where an entity has assets within a number of critical infrastructure sectors, such as communications, data storage and processing and space technology sector.

6. Conclusion

Communications Alliance looks forward to continued engagement with the Department of Home Affairs Critical Infrastructure Centre and all other relevant stakeholders on this important topic.

We share Government's desire to create a robust, effective and efficient framework that appropriately protects Australia's critical infrastructure and systems of national significance.

To the largest extent possible and only to the extent required, this framework ought to build on and enhance existing legislative frameworks and industry efforts.

Our members stand ready to co-design an effective and practical rules framework for the communications and data storage and processing sector.

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