COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Parliamentary Joint Committee on Intelligence and Security
in response to its

Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

1 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 Parliamentary Joint Committee on Intelligence and Security (PJCIS) in response to the Committee's Review of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (SLACIP Bill/Bill).

Communications Alliance also provided feedback to the Department of Home Affairs (DoHA)on the exposure draft of the Bill and engaged intensively and constructively with the Department of Home Affairs leading up to the development of the draft legislation.

We welcome subsequent amendments to the exposure draft, reflected in the Bill, that take account of some of the suggestions that we and our members put forward during this dialogue; in particular the updated definition of 'critical telecommunications asset'.

We remain concerned, however, about other aspects of the Bill and an overall lack of specificity in the Bill. We take this opportunity to re-iterate our feedback that, in our view, has not adequately been incorporated into the Bill nor explanatory material.

We also briefly comment on some of the specific questions suggested for feedback by the Committee under Section 2, *Process and assessment of regulation impact*.

2. Process and assessment of regulation impact

2.1. We welcome the Department's efforts to consult and cooperate with all relevant sectors, including the telecommunications and data storage and processing sectors, in this 'second phase' of the process (after the splitting of the original reform bill into two Bills) as recommended by the Committee.

2.2. However, we do not believe that it was appropriate to conduct the consultation for the exposure draft of the SLACIP Bill over the Christmas holiday period (the exposure draft was released 15 Dec 2021, with submissions due 1 Feb 2022), especially given the additional pressures put on all stakeholders by the Omicron outbreak and other substantial Government-initiated projects, such as the Electronic Surveillance Reform and the requirement for industry to develop Online Safety Code(s). Over-burdening our sector with requests for feedback on complex draft instruments at this time and within such a short timeframe not only denies our staff of much-needed time to spend with family and to 'recharge' but, more importantly, significantly limits the consideration that our members can give to the important issues that the exposure draft of the Bill and explanatory materials raise.

2.3. Equally, the timeframe for introduction of the Bill into the House of Representatives only 10 days after deadline for submissions does not appear sufficient to allow for thorough consideration of the wide-ranging input received.

2.4. Similarly, we fear that this Committee may also not be given the time that is required to adequately consider all input, prior to the Bill being introduced and debated in the Senate.

2.5. As indicated above, we remain also concerned with the lack of specificity in the Bill and the delegation of substance to the rules which are yet to be made.

2.6. We equally highlight our concern with the fact that the Bill is proposed to be enacted without a final Regulation Impact Statement being conducted to assess the far-reaching measures that the Bill imposes on all relevant industry sectors.

3. Statutory review

3.1. The Bill currently does not provide for a statutory review.

3.2. We note that Section 60B of the Security Legislation Amendment (Critical Infrastructure) Act 2021 (the 'first Bill') allows for a review by the PJCIS within 3 years of that Act receiving Royal Assent. **We recommend that the PJCIS make use of its review powers.**

3.3. However, in the context of the SCLACIP Bill, given the broad application of the legislation across different sectors, the lack of specificity in the Bill and the risk of unintended consequences, omissions, the absence of a RIS at enactment, etc., we urgently recommend a statutory review, of the new Act (i.e. the Act that will result from the enactment of the SLACIP Bill) be mandated and scheduled for two years after commencement.

4. Avoidance of duplicative regimes (TSSR / SoCI)

4.1. As previously highlighted, our sector is already subject to extensive security obligations under various other pieces of legislation and regulation, most notably Part 14 of the Telecommunications Act 1997, which contains the assistance requirements of section 313(3) and the security obligations of the Telecommunications Sector Security Reforms.

4.2. We continue to voice our concern that, so far, the telecommunication sector can be subject to duplicative regimes, if the Minister wishes to switch on regulations accordingly.

4.3. In this context, we very much welcome the recent report by this Committee which recommended against any duplication in the two regimes and suggested a highly cooperative approach to determine how this could be achieved.

The Committee recommended:

> *"3.132 The Committee trusts the assertions from government that any potential SOCI obligations will only be 'switched on' if the existing TSSR obligations are assessed as being unsuitable. However, the Committee believes that this decision should be made in consultation with the potentially affected entities and is recommending that that occur through the working group resulting from Recommendation 3."*[1]
>
> *and*
>
> *"Recommendation 3:*
>
> *3.115 The Committee recommends that the Australian Government give consideration to the establishment of a telecommunications security working group comprised of the Department of Infrastructure, Transport, Regional Development, and Communications, the Department of Home Affairs, major telecommunications carriers and carriage service providers, and the Australian Security Intelligence Organisation and the Australian Signals Directorate (when appropriate).*
>
> *This working group could set agreed standards and best practice principles to inform the work of the Cyber and Infrastructure Security Centre's advice and resources."*[2]

We urge the Committee to reiterate its recommendation for the Department of Home Affairs to work with affected entities in a cooperative and consultative approach – that is allowed sufficient time to determine which, if any, obligations of the TSSR regime may require bolstering or amendment and how this may be achieved most effectively and efficiently.

[1] p.49, Parliamentary Joint Committee on Intelligence and Security, Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms, Feb 2022
[2] p.46, Parliamentary Joint Committee on Intelligence and Security, Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms, Feb 2022

4.4. Recommendation 5 of the report of the Committee on the Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms also appropriately highlighted the need for:

> *"establishing a dedicated telecommunications security threat sharing forum, to enable the Australian Security Intelligence Organisation and Australian Signal Directorate to brief telecommunications stakeholders about ongoing and emerging threats to the maximum classified level possible.*
>
> *This forum could be a new group established under the Trusted Information Sharing Network or could be an adjunct group to the existing Communications Sector Group already established under that network, or the working group created as a result of Recommendation 3 of this report.* [3]

It is important to note that this threat sharing mechanism ought to be formalised irrespective of the outcome the consultative approach delivers, to ensure that no duplicative obligations are imposed on our sector. We recommend the Recommendation 5 be reiterated in the context of the SLACIP Bill.

5. Systems of National Significance

5.1. Under Division 2 of Part 6A, the Minister can declare a critical infrastructure asset to be a System of National Significance (SoNS).

5.2. Communications Alliance reiterates its position, made in its submission in response to the Exposure Draft, being:

- that the Bill be amended to require that the Department consults with responsible entities before the Minister gives notice of a proposed declaration pursuant to section 52C, to allow for early input to be provided on accurate identification and importance of their assets.
- the 28-day consultation period concerning a potential declaration of a system of national significance under section 52C is too short, given the highly technical and specialised nature of the assets under consideration. This should be extended to at least 45 days.
- Section 52C should also be amended to provide that the Minister's invitation to make submissions sets out the critical matters on which the submission should focus.
- Proposed section 52B(2) sets out the matters which the Minister must have regard to in determining whether an asset is of national significance. This section should be amended to provide that the Minister must have regard to any submissions provided by the entity responsible for the asset in response to the proposed declaration. As the Bill is currently drafted, it does not provide the appropriate context in which the Minister must consider any submissions received.

6. Protected information

6.1. The Bill includes the fact that an asset is declared under section 52B to be a system of national significance within the definition of protected information.

6.2. Communications Alliance reiterates the following position made in its submission to the Exposure Draft, being:

[3] p.48, Parliamentary Joint Committee on Intelligence and Security, Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms, Feb 2022

- The Bill or the Explanatory Memorandum should be amended to allow entities to disclose the declaration of an asset as a SoNS to relevant entities, such as in its supply chain, when reasonably necessary to comply with its obligations.
- Entities will need to be able to, (subject to relevant confidentiality agreements etc.), disclose the existence of a SoNS declaration to a limited number of parties (e.g. third parties that provide services in relation to the SoNS, vendors, etc.) in order to be able to appropriately protect the SoNS and to prioritise assets and activities accordingly. While the need to disclose such information may arise as a direct result of compliance with the *Security of Critical Infrastructure Act 2018* (SoCI Act) (in which case section 41 appears to permit disclosure), this need may also arise during the course of ordinary business operations and ought to be permitted subject to appropriate confidentiality requirements.

6.3. Importantly, we believe the proposed non-disclosure rules for 'protected information' and/or the definition as to what constitutes 'protected information' are not practical and/or risk to be counter-productive:

6.4. Roughly speaking, the rules operate on two types of 'protected information':

- information described in paragraph (a) of the definition being information "*obtained by a person in the course of exercising powers or performing duties or functions under this Act*"; (Type 1) and
- information described in the rest of the definition including the document and information in a Ministerial Intervention request, annual Risk Management Program report, cyber incident notification, incident response plan, internal evaluation report, external evaluation report, vulnerability assessment report, information gathering direction, action direction, intervention request and such information when the subject of an 'authorised disclosure' (Type 2).

6.5. Section 45 makes it an offence to use 'protected information' except as authorised by sections 41 to 44, all of which relate to disclosures to Government agencies/officials, with the exception of section 43E(3).

6.6. Section 46 creates exceptions to section 45 that appear to aim at accommodating practical uses by the relevant regulated entity. This is supported by a new section 43E dealing with "*authorised disclosure of protected information by the entity to whom the information relates*."

6.7. However, section 43E(3) stipulates that an entity can disclose the 'protected information' Type 1 <u>as long as the information is not also of Type 2.</u> It appears that section 43E(3) is to replace the general exception for use of 'protected information' by the entity itself, the exception that was section 46(4)(b), which is now to be deleted.

6.8. The obvious problem with this is that regulated entities will need to provide a substantial amount of information in the types of reports listed above (see second bullet, section 6,4, i.e. Type 2 information) in order to fulfil their respective security obligations. **Importantly, this information is not unique to the fulfilment of compliance obligations, i.e. this information is necessary for the execution of ordinary business processes and functions. As currently drafted, by using this information for compliance with the requisite security obligations, entities can no longer disclose this information in the ordinary course of business operations. This is not practical and, consequently, not acceptable.** It also risks that those businesses less minded to provide optimal information to Government agencies, may be inclined to minimise the Type 2 information in order to maximise the information they can use for business purposes.

6.9. While the authors of the Bill may argue that section 46(4)(c) creates an overriding exception to 45 for "*the making of the record, or the disclosure or use, of the protected information is in accordance with the express or implied consent of the entity to whom the information relates*", which appears to say that the entity must be able to use and

disclose the information as it sees fit (seeing it can authorise same), this exception does not reconcile well with the general prohibition (by exclusion of use) of section 43E(3).

6.10. Consequently, we strongly recommend that section 43E(3) be deleted and that section 46(4)(b) be retained to allow regulated entities to provide quality information to Government while at the same time continue to operate effectively and efficiently.

7. Data storage or processing service definition and data storage or processing asset definition

7.1. We note that is very difficult to follow the various changes to the *SoCI Act* without a version of the *SoCI Act* that tracks the changes of the 'first Bill' *(Security Legislation Amendment (Critical Infrastructure) Bill 2021*) plus the proposed changes of the SLACIP Bill, and request that such a tracked version be provided for future legislative reform projects.

7.2. It appears that the legislation as introduced intends to repeal the current data storage or processing service definition

> ***"data storage or processing service** means:*
>
> *(a) a service that enables end-users to store or back-up data; or*
>
> *(b) a data processing service."*

to replace it with the following definition:

> ***"data storage or processing service means:***
>
> *(a) a service that:*
>
> *(i) enables end-users to store or back-up data; and*
>
> *(ii) is provided on a commercial basis; or*
>
> *(b) a data processing service that:*
>
> *(i) involves the use of one or more computers; and*
>
> *(ii) is provided on a commercial basis; or*
>
> *(c) a service that is specified in the rules.*
>
> *However, the rules may prescribe that a specified service is not a data storage or processing service.*
>
> *Note: For prescription by class, see subsection 13(3) of the Legislation Act 2003."*

7.3. We also understand that the current definition of critical 'data storage or processing asset' is proposed to be retained.

7.4. Importantly, while the definition of 'critical data storage or processing asset' contains a limitation that the asset must be *"used wholly or primarily to provide a data storage or processing service that is provided by the entity on a commercial basis to an end-user […]"*, the proposed corresponding definition of the 'data storage or processing service' does not contain the limitation that the service be used 'wholly or primarily' to process business critical data, and, therefore, extends the scope inadvertently beyond those services of low systemic risk.

Therefore, we recommend that the definition of critical data storage or processing service be amended to include such a limiting criterion, in line with the current definition of the corresponding asset.

8. Risk Management Programs

8.1. Communications Alliance reiterates the following positions made in its submission to the Exposure Draft, being:

- The Bill should be amended to provide the necessary certainty that the rules made for the purpose of section 30AB applying the risk management program to specified critical infrastructure assets will not take effect for a period at least 6-months from when the rules are made.
- The Bill should be amended to require more extensive consultation (than that provided for in section 30AL) with entities on the detailed requirements that underpin a risk management program to be contained in the rules made for the purpose of section 30AH(1)(c). Communications Alliance recognises that consultation has taken place on draft risk management program rules, however, not all sectors have been involved in this process to the same degree, including the telecommunications sector.
- Section 30AH(6) should be amended to include that in specifying the requirements in rules made for the purposes of paragraph (1)(c), the Minister must also have regard to the input from entities responsible for critical infrastructure assets.

8.2. We also recommend that the standard for compliance with a critical infrastructure Risk Management Program should be set at a reasonableness standard, i.e. an entity would be deemed to comply when that entity has taken 'reasonable steps' to comply with its respective Risk Management Program. This would be consistent with a shared partnership approach to addressing the relevant risks, noting that the Regulation Impact Assessment of the 2020 Bill highlighted that partnerships with industry sit at the foundation of the proposed reforms.

8.3. Further, we believe that the proposal that a rule may be made without consultation in the event of an imminent threat of a hazard having a significant relevant impact on a critical infrastructure asset ought to be accompanied by the expectation of regulatory forbearance in circumstances where the relevant entity has taken reasonable compliance steps. This is so as the lack of preparation and consultation may mean that full compliance is not possible where systems and process changes are required immediately following a rule that has been made under these extreme circumstances.

9. Enhanced cyber security obligations

9.1. Communications Alliance reiterates its position made in its submission to the Exposure Draft being:

- The Bill should be amended to provide that the Secretary's requirement to consult with entities before applying any of the enhanced cyber security obligations in Part 2C should be for a period of at least 28 days. The Bill states only that the Secretary must consult the entity, but does not stipulate any time periods. (See, for example, section 30CB(5).)

9.2. The Bill should be amended so that, before giving notice that any of the enhanced cyber security obligations apply, the Secretary must have regard to any submissions provided by entities in the course of this consultation

10. Access to system information

10.1. The Secretary may require the owner of a critical infrastructure asset, that has been deemed to be a SoNS, to provide "system information" to ASD. This could include real-time telemetry information or periodic reporting, but cannot include personal

information as defined by the Privacy Act 1988. The Secretary would be required to consult with the entity and take account of the cost to the entity of complying with such a request.

10.2. While there is a requirement for the Secretary to have regard to "the costs that are likely to be incurred by the entity in complying with the notice" (section 30DC(4)), and to consult the relevant entity (sections 30DD), there appears to be no independent oversight mechanism.

10.3. Communications Alliance reiterates its position made in its submission to the Exposure Draft, being:

- We would strongly encourage including an independent oversight mechanism to ensure that this power can only be used in extreme situations.
- The Bill should be amended to provide that where a requested entity incurs additional costs in order to meet a request or direction to provide system information, there ought to be a cost-recovery mechanism available.

11. Installation of system information software

11.1. Under section 30DJ of the Bill, the Secretary may require the entity responsible for a System of National Significance to install and maintain a specified computer program to collect and record system information and transmit the information to the Australian Signals Directorate.

11.2. Communications Alliance reiterates its position made in its submission to the Exposure Draft, being:

- This is a very intrusive power, that could require the installation of software against the wishes and advice of the entity in question, and potentially without any prior testing. **We strongly recommend that this power not be included in the Bill.**
- Introducing any software into an IT system without careful coding and testing could result in system disruptions and vulnerabilities being introduced into the system. In the case of complex IT systems run by cloud service providers, improperly vetted software could lead to significant outages and cybersecurity risks, not only to the systems of the cloud service providers, but also to the systems of their customers. Additionally, the mandatory installation of government software on any IT service provider's system would cause customers to doubt the integrity of the IT service provider's services.

12. Conclusion

Communications Alliance looks forward to continued engagement with the Committee and all relevant Stakeholders on completion on these important reforms.

We remain concerned with the lack of specificity in the Bill and urge the Committee to recommend a statutory review within two years of the commencement of the legislation. We are also mindful the Committee's recommendations resulting from its review of the TSSR regime and look forward to a cooperative and consultative approach to determining the best approach to avoiding duplicative obligations for our 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