COMMUNICATIONS ALLIANCE LTD

Communications Alliance submission

to the

Department of Home Affairs

# Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

1 February 2022

## About 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 provide a submission in response to the consultation on the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (SLACIP Bill).

Communications Alliance and its members were deeply involved in the development process of:

- Parliamentary Joint Committee on Intelligence and Security (PJCIS) - *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (TSSR)* (December 2020)
- Parliamentary Joint Committee on Intelligence and Security – Review of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* and Statutory Review of the *Security of Critical Infrastructure Act 2018* (February 2021)
- Department of Home Affairs Critical Infrastructure Centre - *Draft Critical Infrastructure Asset Definition Rules* (May 2021)

**The communications sector is supportive of the objectives of the legislation, but believes that elements of it can and should be improved before consideration by Federal Parliament.**

Our recommended amendments are set out, below.

# 2. Background

In September 2021 the Parliamentary Joint Committee on Intelligence and Security (PJCIS) released its report and supporting recommendations regarding the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Advisory Report).

We recognise that the SLACIP Bill is the second of the two Bills, created in line with the recommendations of the PJCIS.

The second Bill contains a range of proposed amendments to provide for:

- the Risk Management Program under proposed Part 2A;
- enhanced cyber security obligations under proposed Part 2C;
- Systems of National Significance under proposed Part 6A; and
- information sharing provisions for regulated entities.

It should be noted that, although the Department of Home Affairs has said that it will take into account the existing TSSR framework under the *Telecommunications Act 1997*, when considering the risk management program obligation for entities responsible for critical telecommunications entities, there is nothing in the Bill preventing the Government from applying any of the obligations to telecommunications Carriers and/or Carriage Service Providers.

**We believe the Bill should be amended to provide greater certainty on this front, given the risk of duplicative and/or conflicting obligations on industry player to be created.**

# 3. Communications Alliance responses to the Exposure Draft.

The page numbers cited in this document refer to the relevant paragraphs in the Explanatory Document.

## Systems of National Significance p.126.

Under Division 2 of Part 2A, the Minister could declare a critical infrastructure asset to be a System of National Significance (SoNS), triggering the ability of the DHA Secretary to prescribe that one or more cyber security activities be undertaken by the infrastructure owner.

Communications Alliance (CA) Comment: We recommend that the Bill be amended to require that the Department consults with responsible entities before the Minister gives notice of a proposed declaration, 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 proposed new 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.

The Bill 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 responsible entity for the asset in response to proposed declaration.

## Protected information

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

CA Comment: 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 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.]

## Data Storage or Processing Definition and Data Storage or Processing Asset Definition p.29

The exposure draft would amend the definition of a data storage or processing service, adding language to encompass assets such as associated computer systems.

The exposure draft would also amend the definition of a critical data storage or processing asset, adding language to clarify which entities will be captured as responsible entities and that data storage or processing services to Government are captured.

CA Comment: We welcome the proposed inclusion of (d) "is not a critical telecommunications asset" within the proposed amendment to the definition of a critical data storage or processing asset. This appropriately reduces regulatory duplication. However, a potential timing issue remains. Should the "application rules" for the data storage

or processing commence before the passage of the Bill (amending the definition) there is potential for these assets to 'temporarily' be subject to the rules for the data storage or processing sector. We recommend the rules be amended to make it clear that they will not apply to critical telecommunications assets as intended by the proposed amendment to the data storage or processing asset definition.

## Risk Management Programs (RMP) – p.45

The Explanatory Note provide that the Risk Management Program obligations would have a minimum six month delayed implementation, to allow relevant business practices to be aligned.

CA Comment: This statement should be reflected in the Bill itself 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).

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.

## Background Checking p.77

CA Comment: We agree the use of AusCheck should not be mandatory.

## Enhanced Cyber Security Obligations

CA Comment: The Explanatory Note provides that the enhanced cyber security obligations will be considered on a case-by-case basis following consultation with the System of National Significance.

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 and that the Secretary must have regard to any input provided by entities in the course of this consultation.

The Bill should also be amended to include the decision-making criteria the Secretary must satisfy before requiring any owner of an asset declared a SoNS to comply with any of the enhanced cyber security obligations. The criteria should include the costs that are likely to be incurred by responsible entities in complying with the proposed enhanced cyber security obligation.

## Access to System Information p.114.

The Secretary may require the owner of a critical infrastructure asset, that has been deemed to be a SoNS, to provide "system information" to DHA. 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.

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.

CA Comment: We would strongly encourage including an independent oversight mechanism to ensure that this power can only be used in extreme situations.

We also believe 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.

### Installation of Monitoring Software p.120.

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.

CA Comment: 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.

### Other Issues

Definition of **critical telecommunications assets**

CA Comment: The definition as proposed in the exposure draft is unjustifiably broad.

The definition needs to be amended given the inappropriately wide scope of assets captured with the inclusion within the definition of assets "used in connection with the supply of a carriage service". This definition would capture assets such as those used for marketing, sales, and finance purposes that are not connected with maintaining the reliability, availability or integrity of the carriage service.

We suggest simplifying the definition of critical telecommunications asset to:

> ***Critical telecommunications asset*** *means a telecommunications network or facility that is:*
>
> *(a) owned or operated by a carrier or a carriage service provider; and*
>
> *(b) used to supply a carriage service.*

We believe that this simplified definition aligns well with the assets captured under the TSSR and would provide industry with certainty about the scope of critical telecommunications assets captured by the SOCI Act.

## 4. Conclusion

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

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