COMMUNICATIONS ALLIANCE LTD

Communications Alliance submission

to the 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*

22 February 2021

Contents

1. Introduction

Communications Alliance welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Bill) and Statutory Review of the Security of Critical Infrastructure Act 2018 (together: Review).

This submission builds on the feedback previously provided in response to the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (draft legislation).

As with previous reforms in relation to Australia's national security, the communications and data/cloud sectors are keen to assist Government to ensure that Australia's critical infrastructure is secure and resilient in the face of natural disasters and other hazards, and appropriate processes are in place to cope with actual threats to and attacks on our sector's critical infrastructure.

Our sector already has extensive experience in collaborating effectively with Government, security agencies and regulators across a number of regulatory and legislative instruments and frameworks, e.g. assistance provided to law enforcement agencies under the *Telecommunications Act 1997*, the protection of critical infrastructure, including supply chains, in accordance with the Telecommunications Sector Security Reforms, the Data Retention Regime and the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, just to mention a few. Our sector also extensively engages with emergency services organisations and Federal Government and State/Territory departments in relation to natural disasters and the COVID-19 pandemic.

We are conscious that the protection of critical infrastructure is a national priority and, as such, must also be tackled through a collaborative and principles-based approach across all sectors and stakeholders. Overall, Australia's cyber security policies ought to be guided by a number of principles. These policies should:

- Be risk-based, flexible, robust, embrace collaboration and promote innovation-friendly and technology-neutral solutions;
- Foster voluntary public private partnerships, as collaboration is and will continue to be essential to build effective cyber resilience;
- Draw on existing, interoperable and global best practices and voluntary industry standards and certifications that improve security while enabling growth in international commerce through digital means;
- Be based on principles rather than prescriptive measures; and
- Raise awareness to citizens, public and private sectors on how to lower their cyber security risk through proper online practices.

The telecommunications sector is already subject to security obligations under the Telecommunications Sector Security reforms (TSSR). This is a well-established and robust security regime that has successfully achieved an uplift in security across the sector and improved engagement with Government on security matters.[1] We submit that any changes to further enhance security objectives in the telecommunications sector would be best achieved by amending that regime.

[1] Department of Infrastructure, Transport, Regional Development, and Communications, *Submission Parliamentary Joint Committee on Intelligence and Security (PJCIS): Review of the operation of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms*, pp.7-8.

Given the interlocking nature of the TSSR and the Review and the potential for duplication, friction or even conflict arising from the two regimes – which are currently both before the PJCIS – we would welcome an opportunity for further discussion and input once the Committee has made further progress in its respective inquiries.

2. Process

The Bill takes a deliberately broad approach to additional or enhanced national security obligations for eleven critical infrastructure sectors. As we understand it, the rationale for this approach is to allow for a more detailed analysis of existing legislative and regulatory requirements as they pertain to the respective sectors in a sub-ordinate process, and to, subsequently, only 'switch on' the obligations contained in the draft legislation on a sector or even asset-specific basis where gaps in already existing sector-specific requirements have been identified.

Where this is the case, the obligations contained in the Bill would be underpinned through more detailed rules which, so we have been assured, would be developed through highly cooperative and sector-specific processes. While this approach may be appealing in theory, it makes it very difficult for our sector (and most other sectors, so we imagine) to provide detailed feedback at this stage in the process, because members are unable to develop an understanding of the actual obligation as they apply to their individual organisations and assets.

We also note that this approach stands or falls on the basis that there will be a genuinely cooperative process for any gap analysis and further rule development. Such a process must be allocated sufficient time and cannot be governed by unrealistically tight timeframes. At the time of writing this submission, the time allocated for the co-development of sector-specific rules was given with 8-10 weeks. This appears too short given the complexities involved.

Given the importance of the sector-specific rules for the success of the entire framework, we believe that the details of the foreshadowed consultative process for the co-design of those rules ought to be clearly spelled out and established. This should include objective criteria set out in the legislation for the making and amendment of sector-specific rules and an ability for affected entities to seek review of the way in which the rules apply to them and the critical infrastructure assets for which they are responsible.

While the Department of Home Affairs has said it will develop a planned timeline for the co-design process, this is only one important dimension of the problem. The more significant dimensions are what these obligations will look like in practice, to whom they will pertain and to which assets they will be applied? Which assets will form a system of national significance (SoNS)? How will they be described and specified? How will sectoral overlap be dealt with? Without knowledge of all these dimensions (and these are just a few) it is impossible to calibrate the impact of the proposed obligations, or to properly understand how they will function and whether other improvements or safeguards are needed – or indeed whether the proposed regime meets regulatory best practice.

Consequently, we recommend that the Committee advise Parliament that further consideration of the Bill ought to be deferred until Government has produced a reasonably detailed outline of the end-state of the reforms. That is, an outline indicating what is the scope of assets, specific obligations, resulting outcomes etc. that Government expects to see for each sector once it has made use of the delegated powers contained in the Bill.

We appreciate Government's intention to co-design the rules framework and our request for a detailed outline of the end-state of the reforms ought not be misunderstood as a rejection to intensively and cooperatively work with all stakeholders as part of the reform process. However, in order to be able to determine whether the proposed Bill and reform represents indeed the best way forward, in terms of costs and benefits and in terms of meeting the security challenge, we believe far more detail is required at this stage, and this detail ought to be brought before Parliament.

The Standing Committee for the Scrutiny of Bills raised a similar point when it raised concern with the range of powers that the Bill seeks to insert to prescribe matters in delegated legislation.

> *"The committee's view is that matters which may be significant to the operation of a legislative scheme should be included in primary legislation unless sound justification for the use of delegated legislation is provided. The committee considers that these matters have not been sufficiently addressed in the explanatory memorandum and that the prescription of so many delegated legislation making powers in the bill has not been adequately justified.*
> ***The committee therefore requests the minister's detailed advice as to why it is considered necessary and appropriate to leave each of the above matters to delegated legislation."***[2]

Irrespective of the difficulties highlighted above, we are concerned that the Bill will introduce overlapping and duplicative obligations for the communications sector in different pieces of legislation, such as the TSSR, *Telecommunications Act 1997*and the *Security of Critical Infrastructure Act 2018* (SoCI Act). At best, the result would be a framework with distinct obligations contained in various pieces of legislation and regulation – a situation which appears likely to create operational inefficiencies for all stakeholders involved.

As we will highlight further below, we are also concerned with duplicative and/or conflicting requirements that could arise from within the rules framework of the proposed new regime itself but also from the co-existence of the new regime and already existing regimes in the date storage and processing sector.

Against this background, we offer the following observations.

3. Breadth of obligations

Noting, the various 'on-switches' that may trigger different obligations, it would appear that all telecommunications Carriers/Carriage Service Providers (C/CSPs) and cloud/data providers are likely to be captured by the draft legislation. This, in combination with the very broad definitions of 'data storage and processing provider/service', creates extensive reach, consequent industry-wide compliance costs and potential for duplication of efforts across the sector. (Also refer to Section 5 for further thoughts on duplication of regulations.)

The legislation should consider whether certain types of providers or services can be excluded from the obligation at the outset, rather than accepting default inclusion of all C/CSPs (and subsequent 'on-switches' via asset categories or SoNS). This could be done through nominating specific C/CSPs (as occurs in regard to the notification obligations of TSSR regime) or by exempting certain types of C/CSPs (e.g. as a function of size/subscriber/type of customer/numbers). Similar treatment could be considered for cloud/data sector providers.

The definition of 'asset' is very broad – in fact the 'definition' is a non-exhaustive list of items that may be considered an asset instead of a clear definition of the term. Importantly, the term 'critical telecommunications asset' is almost as broad in that the only criteria of such a classification are ownership or operation by a C/CSP, or 'use [of the asset] in connection with the supply of a carriage service'. While we agree that it is indeed the use that is likely to determine the criticality of an asset (among other things), the requirement of a mere 'use in

[2] p. 21 Scrutiny Digest 2/2021, Standing Committee for the Scrutiny of Bills

connection with the supply of a carriage service' casts the net so wide that almost every asset in our sector is, by definition, a critical telecommunications asset.

This ought to be addressed by determining an appropriate threshold for criticality similar to the threshold set in section 9(3) of the current SoCI Act which lists a number of criteria that the Minister must satisfy him/herself of prior to declaring an asset as critical that is not yet part of the listed critical infrastructure assets.

Without further limitation on the types of assets that can be subject to (yet to be developed) rules, it will be difficult for our sector to be confident that duplication will or even can be avoided during the rule-making process.

4. Definition of Critical Data Storage and Processing Assets

We welcome the omission of the reference to commercial services in the definition of 'data storage or processing sector', 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.

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.

5. Duplication/costs and operation of parallel regimes

TSSR:

Industry notes that the August 2020 consultation paper had flagged an intention for a positive security obligation (PSO) to be implemented through "sector-specific standards proportionate to risk".[3] The Bill imposes three types of (separate) PSO for critical infrastructure assets of responsible entities, where the asset is subject to rules made under section 61 of the SoCI Act or the asset has been subject to a declaration as per section 51 of that Act. Where such rules (or a declaration) have been made, it appears that a C/CSP is required to maintain and annually report against risk management program(s) which encompass all infrastructure assets of a C/CSP. This, in and by itself, is a substantial compliance burden with attendant costs.

In addition, nominated C/CSPs have the option (under TSSR) to develop and submit an annual security capability plan or to incrementally notify any planned changes to infrastructure that could compromise their capacity to comply with the security obligation of section 313 of the *Telecommunications Act 1997*. That is, the regime envisages either an annual plan or incremental notifications, but not both. Given that the characteristics of a security capability plan appear analogous to the description of critical infrastructure risk management plan as set out in the Bill, a consistent approach which would avoid substantial duplication of effort for both providers and the Critical Infrastructure Centre would be to remove the TSSR notification obligation for critical infrastructure providers which are subject to the PSO and the requirement to develop, maintain, keep up to date and report annually

[3] Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper,* August 2020, p10.

against a critical infrastructure risk management plan. The potential co-existence of the new PSO, especially the proposed risk management programs, and the TSSR obligation in relation to capability plans and notification would likely create an unnecessarily heavy compliance burden, overlap and duplication which Government sought to avoid.

Aspects of the PSO are already captured by the section 313 requirements of the *Telecommunications Act 1997* to do one's best to prevent unauthorised access to and interference with networks and facilities owned or operated by a C/CSP. It appears that this higher order requirement now has been overlaid with additional (as we believe unnecessary) prescription through the draft CI SoNS legislation requirement (where 'switched on') for a risk management plan and associated reporting.

The telecommunications sector already has a mature cyber security posture, which has been enhanced by the TSSR. C/CSPs have undertaken substantial (and costly) work to comply with the TSSR obligations, i.e. obligations which are the Critical Infrastructure Centre describes as follows:

> "*Security obligation: All carriers, carriage service providers and carriage service intermediaries are required to do their best to protect networks and facilities from unauthorised access and interference – this includes maintaining 'competent supervision' and 'effective control' over telecommunications networks and facilities owned or operated by them.*
>
> *Notification obligation: Carriers and nominated carriage service providers are required to notify government of planned changes to their networks and services that could compromise their ability to comply with the security obligation."*[4]

Given that C/CSPs have an obligation to keep networks secure, maintain 'competent supervision' and 'effective control' and to notify Government (and receive approval) of any potential changes that may compromise this ability, it appears that another obligation to maintain risk management programs is duplicative of the efforts that C/CSPs already must have in place in order to be able to comply with the TSSR/section 313 requirements. In other words, if critical infrastructure assets are already secured to a C/CSP's best ability, why is another similar layer of risk management required? If Government considers the existing TSSR regime to be deficient, we submit the best way to achieve improved security outcomes for the telecommunications sector would be to amend the TSSR to address these (actual or perceived) deficiencies. Applying additional overlapping obligations via the SoCI will increase compliance costs without necessarily improving security outcomes.

The security of Australia's telecommunications networks is a critical concern for all C/CSPs. There is an ongoing need for investment in telecommunications networks in Australia, and so we believe, industry is best placed to manage its networks, including securing them, if it has appropriate information to do so. The two-way exchange of information facilitated by the TSSR improves the ability of C/CSPs to effectively manage risk as it pertains to their networks.

Assuming that the critical infrastructure asset subject to the rules of the SoCI Act that trigger the obligations to develop and maintain a risk management plan apply to a type of asset that forms part of all C/CSPs' infrastructures, the requirement for any C/CSP to effectively audit and report against all of a C/CSP's infrastructure, instead of developing capability plans or incrementally providing notification of changes to infrastructure where this may compromise the capacity to comply with the security obligations of section 313 by nominated CSPs, appears to create further duplication.

---

4 As accessed on 26 November 2020: https://cicentre.gov.au/tss/about

If a PSO, including an obligation to maintain and report against critical infrastructure risk management plans, was indeed to be applied to all C/CSPs (as appears likely due to the breadth of the definitions of asset and critical telecommunications asset), then it appears that the TSSR capability plan/notification requirements would be duplicative and, therefore, should be rescinded. That is, section 314A of the *Telecommunications Act 1997* and the associated provisions which support its operation ought to be removed from that Act.

Alternatively, the SoCI Act could include a requirement that the Communications Access Co-ordinator (CAC) provide an exemption to a responsible entity from the TSSR notification requirements of section 314A(1) of the *Telecommunications Act 1997* where the Minister has determined (under the SoCI Act) that the entity's asset will be subject to the PSO (risk management program). Section 314A(5A) of the *Telecommunications Act 1997* already contains powers for the CAC to grant such exemptions.

We also caution against the sheer volume of information that Government would be required to process if it actually wanted to assess the material that C/CSPs have already produced – which would be further augmented where a PSO has been notified – as part of their standard risk management processes.

Lastly, we note that the Australia's Cyber Security Strategy 2020 indicated that enhanced threat sharing between security agencies and industry, i.e. threat sharing in both directions, forms a key component of the Strategy. We believe that it is timely to add a threat sharing obligation for security agencies analogous to the requirements placed on critical infrastructure owners.

Data Storage and Processing:

Given the naturally wide scope and use of data storage and processing in the digital environment, the Bill has the potential to create substantial regulatory overlap between regulations for the data storage and processing sector and the regulations of any (or all for that matter) of the eleven other critical infrastructure sectors.

The potential for overlap for the data storage and processing sector is substantial if the end-user of a data storage or processing asset is a regulated critical infrastructure entity in one of the other regulated sectors that is storing or processing 'business critical data' (or is a public sector end-user). This scenario appears indeed highly likely.

As almost any critical infrastructure sector has entities that use the same data storage and processing services as entities in other sectors, it is almost unavoidable that the data storage and processing sector could become subject to the regulations of all critical infrastructure sectors in parallel – a situation that is clearly not useful, nor practical or economical.

Therefore, it is critical that the legislation (as opposed to the rules framework) enshrines clear rules that ensure that no unnecessary overlap can occur. One way of doing so would be to ensure that a regulated entity is only ever required to comply with one set of sector requirements for a respective asset. For the data storage and processing assets this must mean that an asset's compliance with its own sector's PSO would be considered meeting all other sectors' PSOs that require security reviews etc. from data storage or processing service assets.

Given the enormous complexity of the overlap of this sector with all other critical infrastructure sectors, we believe far more work is required at this early legislative stage. Similar to our request in Section 2 above, we recommend that the Committee defer consideration of the Bill until Government has provided significantly more detail on how it intends to resolve the issues of overlapping regulations, existing and future.

6. Cost of compliance

We encourage Government to set out a legislative basis for limiting and/or apportioning the costs of compliance with notices and directions in a manner that is scalable to the size of the entity. Cost recovery should also be available for entities in certain circumstances where costs are incurred (e.g. as a result of damage to property or systems) due to Government intervention. We consider it important that the critical infrastructure reforms preserve the principle of cost recovery, which is well established under the *Telecommunications Act 1997*, for example where C/CSPs provide assistance under section 313 of that Act.

7. Systems of National Significance – definition and secrecy requirements

Industry struggles to understand which parts of their infrastructure (if any) would be considered a SoNS. Given that all C/CSPs and cloud/data providers appear to be covered by the legislation, it does not appear possible to exclude certain infrastructure or systems from the 'catalogue of potential options'. In the case of the telecommunications industry, there is an extensive range of both communications and supporting IT systems at a variety of layers across both mobile and fixed line networks and content layers, all of which may be directly or indirectly involved in the provision of 'business critical data' which could trigger a notification.

The criteria of 'interconnectedness' and that a SoNS must be a 'system' do not offer much guidance, as neither term is defined in the Bill and their common sense or dictionary definitions are very broad and/or variable depending on the perspective of the person considering the matter. The terms do not take into consideration the complexities of the telecommunications industry.

The proposed 28-day notice and consultation period for a declaration of an asset as a SoNS is rather short and, consequently, we recommend that the Minister and Department engage with the respective asset owner as early as possible (and well before the formal notice period) in order to allow all stakeholders to gain a detailed understanding of the highly technical and specialised nature of the infrastructure system under consideration.

Moreover, we are still unsure whether the arrangements for authorisation and disclosure of the existing section 41 of the SOCI Act are sufficient for our sector:

The definition of 'protected information' includes "a document or information that records or is the fact that an asset is declared under section 51 to be a critical infrastructure asset". Section 41 of the SoCI Act allows disclosure of protected information "if the entity makes the record, or uses or discloses the information, for the purposes of: (a) exercising the entity's powers, or performing the entity's functions or duties, under this Act; or (b) otherwise ensuring compliance with a provision of this Act." The note accompanying this section indicates that "This section is an authorisation for the purposes of other laws, including the Australian Privacy Principles."

We seek clarification that the non-disclosure provisions for protected information, including information of the fact that an asset has been declared a critical infrastructure asset and/or a SoNS, do not impede operational effectiveness and efficiency of the respective responsible entities. 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.

Similarly, it would appear inefficient (or even ineffective) for suppliers of services to SoNS to be 'kept in the dark' of the importance of the services that they render in a national security context.

This approach also seems to conflict with the recently proposed transparency principles set out in Government's *Critical Technology Supply Chain Principles*, and in particular the advice to entities that "understanding your suppliers and networks ensures your organisation is aware of these [security] risks, can identify bottlenecks, and then determine alternative sources of critical inputs when needed."[5] Industry would appreciate further guidance on how these two aspects are envisioned to operate alongside each other.

8. System information software notice

Section 30DJ allows the Secretary to require the owner of a SoNS to "install a specified computer program on the computer", to maintain that program and keep it continuously connected to the internet.

As SoNS may not necessarily clearly segregate network and system data from other data, including data that relates to customer activities, customers' use of products and services, network data relating to end-users etc., such security monitoring software may unintentionally also scan data that ought not be subject to such activity.

The operation of such software on a SoNS may also be inconsistent with the requirements and prohibitions of overseas legislation, including the EU and US, and the laws of other jurisdictions may apply to the specific global provider of a service. This is particularly true for providers of cloud solutions.

Furthermore, the adoption of third-party software in a cloud environment without appropriate security reviews and procedures may be increasing security risk rather than mitigating the risk.

Importantly, it ought to be understood that the roll-out of such software and its continued operation may be very costly. These costs ought to be borne by Government and must not be considered as a 'cost of doing business' for SoNS.

At a minimum, the scope of the system information software notice requirement should be narrowed to exclude providers of cloud services and operators of cloud data centres.

9. Rule-making/amendment powers

Section 61 of the SoCI Act allows the Minister for Home Affairs to make, by legislative instrument, rules required or permitted by the Act or rules "necessary or convenient to be prescribed for carrying out or giving effect to [the] Act". The proposed new Section 30AL of the SoCI Act stipulates a 28-day consultation period (which commences with publication of the draft rules on the Department's website) which does not apply if the Minister is "satisfied

[5] Australian Government, *Critical Technology Supply Chain Principles: A call for views*, p10, September 2020

that there is an imminent threat that a hazard will have a significant relevant impact on a critical infrastructure asset" or where such a hazard had or is having such an effect.

These consultation requirements are not appropriate for the following reasons:

The retrospective consideration of hazards in combination with the ability to forgo consultation on the grounds that a hazard had a significant relevant impact in the past effectively means that the Minister could make a rule without consultation so long as the rule covers a type of hazard that previously had the required impact. The provision ought to be amended to ensure, at the very least, that a retrospective consideration of a hazard cannot constitute grounds for dispensing with the consultation requirement. It is hard to see how a past event would create an urgency that would justify this measure.

We recognise that the Bill now includes a consultation period of 28 days (previously 14 days). However, we believe that this period is still very tight to allow for a cooperative and meaningful consultation on what are likely to be detailed rules which may require a high degree of technical expertise for a considerate analysis. We note that section 378(5) of the *Telecommunications Act 1997* stipulates that for technical standards – which are likely to be similar in nature and consultation needs to the rules contemplated under the SoCI Act – a period of at least 60 days constitutes "an adequate opportunity to make representations". Consequently, we request that the consultation period of section 30AB of the Bill be extended to 60 days.

Independent of the above, we note that section 125AA of the *Telecommunications Act 1997* already provides for an opportunity for the Minister of Communications, Cyber Safety and the Arts to direct the regulator, the Australian Communications and Media Authority (ACMA), to make standards. Where so directed, the ACMA must determine a standard in compliance with the details of the direction given by the Minister.

We believe that the existing standards, making powers by the portfolio Minister ought to be the primary means by which 'rules' pertaining to the sector ought to be made as it is likely that the industry regulator's expertise in relation to the operation of the industry is well suited – in cooperation with the Department of Home Affairs – to translate the desired outcomes into practical, efficient and effective industry regulations.

10. Definition of National Security

Section 5 of the SoCI Act defines national security as "Australia's defence, security or international relations". This definition is broad and does not limit national security to any specific activities. However, the definition of national security is key to the operation of the Bill, including the rule-making powers, the Ministerial declaration powers and the far-reaching directions powers. Importantly, the Explanatory Document to the Bill cites national security concerns as the primary reason for exempting the Ministerial authorisations under Part 3A of the Bill from judicial review under the *Administrative Decisions Judicial Review Act 1977*.[6]

Given the wide scope of the current national security definition and the intrusive nature of the powers (and attendant penalties for non-compliance), we urge Government to adopt a more narrow definition which ties national security to specific activities, conducts and interests. The current definition of national security under section 90.4 of the *Criminal Code Act 1995* might provide a useful approach. Alternatively, it is also worth noting that section 5 of the SoCI Act already includes a definition of security which references the definition of the

[6] Department of Home Affairs, *Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020,* November 2020, p. 65

Australian Security Intelligence Organisation Act 1979 (ASIO Act). The latter, in turn, includes more specificity on the activities that could be considered a threat to Australia's security. Therefore, the ASIO Act definition of security would also be preferable to the definition of national security of section 5 of the SoCI Act. In fact, it is hard to see why a separate definition of national security is required given the existing (and referenced) definition of security in the ASIO Act.

If the definition of national security was to be retained, at the very least the individual terms that make up the definition of national security, i.e. 'defence', 'security' and 'international relations', should be defined within the legislation rather than be left to their ordinary meaning. In this context, section 10 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* may offer a useful reference point which would also provide consistency with Australia's commitments to the United Nations Norms of Responsible State Behaviour in Cyberspace.[7]

11. Ministerial authorisations and directions powers

The Bill allows the Minister to authorise agencies to direct responsible entities, under certain conditions, to provide information, perform a certain action and for agencies to intervene in the operations of a critical infrastructure asset.

While we recognise the need for Government agencies to be able to act swiftly in a crisis, we are also mindful of the risks and potential unintended far-reaching consequences that accompany the powers proposed in the Bill. As currently drafted, we believe the directions powers are disproportionate to the risk that they pose and, consequently, they ought to be amended. In this context, we note that the new reference to the Ministerial power to issue an authorisation when an emergency has been declared under the *National Emergency Declaration Act 2020* is welcome but exists in parallel to the other Ministerial authorisation powers. Therefore, the reference as such does not address our concerns.

Given the far-reaching nature of the directions powers authorised by the Minister, the criteria that the Minister must consider prior to making authorisations ought to set a high threshold and ought to be comprehensive.

We raise the following concerns with the current Bill in this regard:

Similar to the considerations contained in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and/or section 315B of the *Telecommunications Act 1997*, these considerations ought to include, in addition to the considerations already included in the Bill:

- the legitimate expectations of the Australian community relating to privacy and cyber security;
- whether the action proposed for a direction constitutes the least intrusive means of dealing with the cyber incident;
- the relative impact to other entities that may be adversely affected by the direction to the responsible entity; and

[7] As accessed on 26 November 2020: https://www.dfat.gov.au/international-relations/themes/cyber-affairs/international-security-and-cyberspace).

- the legitimate interests of the responsible entity to whom the direction relates, including the costs, in complying with any direction, that would be likely to be incurred by the responsible entity.

Importantly, the Minister ought only to be permitted to consider authorising a direction unless he/she has received an adverse security assessment in relation to the incident and the asset under consideration. The adverse security assessment in turn ought to be a key item for the Minister to have regard to when contemplating the making of an authorisation.

It also appears that the authorisation/directions powers, as currently drafted, do not expressly consider a process of exchange on the technical feasibility – and potential unintended consequences – of requests between the Minister/agency and the respective entities, especially with respect to intervention directions.

We note that technical feasibility and other matters form part of the criteria that the Minister has to consider prior to giving his direction. However, we believe the process could be improved by including an express requirement to give the entity an opportunity to either comply with a direction and/or to respond with potential objections. Only once this process has taken its course, should the Minister be allowed to authorise a direction (subject to other requirements being fulfilled).

Importantly, it is not clear from the Bill to what extent the Minister has received specific details about the type of actions or interventions that are believed to be required prior to making the Ministerial Authorisation. Without sufficient detail, including technical specifics, as to what is being contemplated, the effectiveness of consultation with the respective entity (as required prior to the making of a Ministerial Authorisation) will be very limited. It is concerning that the Bill appears to allow for a 'blank cheque' (within the constraints of the matters that the Minister needs to consider prior to making an authorisation) for agencies to request far reaching actions or intervene with the operations of an asset. The Bill ought to be amended to expressly require security agencies to provide the Minister with a detailed technical 'plan' as to how they propose to address a specific incident and why this 'plan' is suggested above other available options, that this 'plan' be shared during the mandatory consultation and that the direction be very specific and limited to the means included in the 'plan' that has been put to the Minister.

We are also conscious of potential diverging views between the Minister/agencies and responsible entity subject to a direction as to whether a responsible entity was "unwilling or unable take all reasonable steps to resolve the incident": a responsible entity may well be willing and able, in its view, to resolve the incident but would do so through means that agencies may find inappropriate, or resolve the incident to an extent that agencies may consider 'incomplete' or not satisfactory. While this inherent tension will be difficult to resolve without independent review of proposed authorisations/directions (refer to our comments further below), we believe that more detailed and express consultation requirements with respect to technical feasibility and increased requirements on the specificity of authorisations would assist with ameliorating some of these concerns.

We also raise concern that the consultation requirement contained in section 30AB is significantly weakened by the limitation that such consultation is not required if the delay introduced through consultation would frustrate the effectiveness of the Ministerial authorisation. It is easy to see that almost any consultation would introduce delay and that delay may reduce the effectiveness of an action given the time critical nature of many incidents. As drafted, even a short delay and marginal reduction in effectiveness would allow the Minister to proceed without consultation. Therefore, we recommend that the threshold for this limitation be raised by requiring that a 'substantial delay' would 'substantially frustrate the effectiveness' or words to a similar effect.

12. Independent assessment/judicial review

The Bill exempts decision under Part 3A of the SoCI Act from potential judicial review under the *Administrative Decisions (Judicial Review) Act 1977*. While intervention directions – but not the information gathering directions and action directions – require approval of the Prime Minister and the Defence Minister, we are concerned that the framework as proposed does not include appropriate safeguards for independency and review.

In our view, it would be beneficial for the authorisations to be subject to ex-ante (and speedy) review by an independent body. This could be achieved through the implementation of the recommendation made by the Independent National Security Legislation Monitor (INSLM) in its Report *TRUST BUT VERIFY, A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters* to establish an Investigative Powers Commission – it appears that the underlying issues and powers contemplated in the Bill and already granted by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* are very similar in nature and would warrant a similar approach.

Including an adverse security assessment as a prerequisite for all Ministerial authorisations of directions would also allow the responsible entity to apply for review through the Security Appeals Division of the Australian Appeals Tribunal (AAT) and would align the SOCI Act with the existing requirements of Part 14 of the *Telecommunications Act 1997*.

.

13. Conclusion

Communications Alliance looks forward to continued engagement with the Committee, the Department of Home Affairs and 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. A thorough and evidence-based gap analysis is required to ensure the reforms are not duplicative or, worse, contradicting existing frameworks.

Our members stand ready to work with Government and all other relevant stakeholders to create a practical, effective and proportionate framework in a realistic timeframe.

For any questions relating to this submission please contact [redacted] on [redacted]

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