Communications Alliance

Response to Questions on Notice

PJCIS Hearing 20 May 2021

Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms

1. **Mr DREYFUS:** Thanks, Mr Stanton. In addition to potential duplication, the Law Council, at paragraph 8 of its submission, has identified a number of inconsistencies between the telecommunications sector security reforms, TSSR, and the proposed expansion to the security of critical infrastructure regime. An example is the Law Council noting that, under the TSSR, most regulatory responsibilities are performed by the critical access co-ordinator and that numerous staff can be appointed to that position, including all staff at the executive level 1 and 2 classifications. By contrast, the equivalent regulatory functions under the proposed revisions of the Security of Critical Infrastructure Act would be conferred on the secretary of the department and could only delegated to senior executive service levels. In other words, there's a significant difference in the seniority of the persons who may be authorised to perform the same or substantially similar regulatory functions. Can you see any justification for that inconsistency? Do you have observations or concerns that you'd like to share about that issue? For example, would it be your view that these sorts of regulatory functions should only ever be performed by the senior executive service level public servants?

Response

The proposed amendments to the *Security of Infrastructure Act 2018* (SoCI Act) appear to have been drawn up in isolation and without detailed consideration of the existing TSSR obligations and/or how new and existing provisions should interact. This will necessarily lead to the types of inconsistencies identified by the Law Council. For example, both TSSR and the SoCI Act proposal have information gathering and directions powers but they have different thresholds for use, and decision making is delegated to different levels within the public service. Ideally the frameworks would be considered together, and a comprehensive set of reforms proposed without these types of inconsistencies.

We support the Law Council's recommendation for a comprehensive review of the proposed revisions of the SoCI Act and their workings with the TSSR.

In response to the specific question on the level of executive delegation (under TSSR) versus senior executive level delegation (under the SoCI Act proposals) we would note that, in some cases, the functions being performed are different and, therefore, a different level of delegation might be appropriate. Under the TSSR executive level 1 and executive level 2 staff have some delegations (related to assessing security notifications and providing security advice in response), but do not have the delegation for use of the information gathering or directions powers. A comprehensive review of the proposed SoCI Act proposals and the TSSR obligations would be the best way to tease these issues out.

As a matter of principle, we believe where any additional requirements and powers currently contemplated under the SoCI Act proposals were to be brought under TSSR, then the seniority of delegation ought to reflect this, i.e. only more senior personnel ought to have information-gathering powers and/or regulatory responsibilities.

2. **Mr DREYFUS:** That would be helpful; thanks, Mr Stanton. A related point is a Law Council observation, at paragraph 8 of their submission, that the information-gathering powers under the TSSR may only be delegated by the Secretary of the Department of Home Affairs to the Director-General of Security. By contrast, the Security of Critical Infrastructure Bill would allow the secretary to delegate similar information-gathering powers to any SES-level employee at the department. Probably you will want to take this on notice, but I'd be interested in any observations you've got about that difference. It goes to whether these sorts of intrusive powers should only be ever exercised by officers with the status and seniority of the Director-General of Security. Perhaps rather than answering now, you could take that on notice.

Response

The current requirements for the delegation of powers as set out in the TSSR, i.e. the information-gathering powers can only be delegated to the Director General of Security, is appropriate and ought to be retained. As indicated in our testimony before the Committee, our preference is to retain the TSSR and, if required at all, to add any 'missing components' to that regime rather than creating parallel regimes or 'moving the TSSR into the SoCI Act'.

If the latter two scenarios became a reality (two parallel regimes or 'TSSR moved into SoCI Act'), then the requirements for delegation of powers with respect to information-gathering powers currently contained in the TSSR ought to be replicated in the SoCI Act.

3. **Mr DREYFUS:** On another point, noting that Commonwealth officials are able to use and disclose information obtained from telecommunications providers under the telecommunications sector security reforms for the purposes of security within the meaning of the ASIO Act, the Law Council has raised a concern that the definition of 'security' is too broad. That's at paragraphs 11 to 19 of the Law Council's submission. The Law Council is suggesting that it might be too difficult for providers to comply with their obligations under part 14, including the obligation 'to do one's best' to protect their networks and assets from security threats because the definition of security extends far beyond the ordinary meaning of the term. So an example would be that the term 'politically motivated violence', which forms part of the definition of security, is capable of covering legitimate protest and dissent, including the actions of people who do not engage in violence but whose activities may attract counter protesters who do engage in violence. Is that breadth of the definition of 'security' a concern to the Communications Alliance? And, if it is, would you have thoughts on how that concern could be addressed?

Response

Our members have not raised any concern about the inclusion of 'politically motivated violence' as one of the examples of national security risks.

However, our members are concerned that different pieces of legislation that strongly relate to or the sole purpose of which it is to strengthen national security, do not adopt a single, well-defined definition of 'national security'.

How are critical infrastructure organisations across different sectors supposed to implement a risk-based approach to national security compliance when the definitions of 'national security' in different pieces of legislation that these organisations are subject to are not identical, let alone consistent?

Any additional confusion or ambiguity introduced due to variations in definitions unnecessarily adds to the risks and resources that need to be employed and managed by industry and government, and ought to be eliminated.

While we acknowledge that the implementation of the recommendations of the Richardson Review may target some of these inconsistencies, we recommend ensuring that existing opportunities, such as the review of the SoCI Act, be used to harmonise the definition of 'national security'.

We have previously commented (in our submission to this Committee in Feb 2021) on the proposed definition of 'national security' in the SoCI Act and have reproduced our response below for your convenience.

Extract from the 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*

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*.[1]

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 *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.[2]

---

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

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