Law Council
OF AUSTRALIA

Supplementary submission:

Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

6 July 2021

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2021 Executive as at 1 January 2021 are:

- Dr Jacoba Brasch QC, President
- Mr Tass Liveris, President-Elect
- Mr Ross Drinnan, Treasurer
- Mr Luke Murphy, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

The Chief Executive Officer of the Law Council is Mr Michael Tidball. The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council of Australia gratefully acknowledges the contributions of the following members to this supplementary submission:

- members of the Business Law Section, and in particular, members of the Corporations, Privacy and Foreign Investment Committees; and
- members of the National Criminal Law Committee.

Executive Summary

1. On 11 June 2021, representatives of the Law Council of Australia appeared before the Parliamentary Joint Committee on Intelligence and Security (**Committee**) at its public hearing in relation to the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**SOCI Bill** or **Bill**).

2. This supplementary submission provides the Law Council's response to four matters taken on notice at the hearing. It also provides some further submissions on aspects of the proposed governmental intervention powers in responding to serious cyber security incidents affecting critical infrastructure assets in new Part 3A of the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**).

Questions taken on notice

3. Representatives of the Law Council took four matters on notice, as follows:

   (1) **technical issues concerning new Part 3A**—Law Council representatives offered to provide further information about technical issues in relation to the intervention powers in proposed Part 3A, which are as follows:

   (a) the absence of a provision requiring the Australian Signals Directorate (**ASD**) to provide regulated entities with an inventory of actions taken in relation to their computers (such as altering or deleting data, or otherwise interfering with the functioning of a computer) while carrying out an intervention request issued by the Secretary of the Department of Home Affairs under new Part 3A; and

   (b) a potential lack of clarity for 'end users' of the legislation in relation to the purported prohibition on ASD taking offensive cyber action pursuant to an intervention request;

   (2) **limitations in immunities conferred on regulated entities and their individual personnel**—Senator the Hon Kristina Keneally asked the Law Council to elaborate on the basis for its recommended amendments (in recommendation 34 of the Law Council's main submission) to address limitations in immunities for regulated entities under the expanded regime;

   (3) **expansion of SOCI regime to supply chains**—Senator David Fawcett sought the Law Council's views on whether the SOCI regime could be further expanded in the future, beyond the 11 sectors in the Bill, to comprehensively address the issue of 'supply chain reliance'. For example, Senator Fawcett questioned whether there is a need for specific regulatory coverage of pharmaceutical supply chains which service 'critical hospitals' as is proposed to be defined in section 5 of the SOCI Act (item 7 of Schedule 1 to the Bill);

   (4) **consultation with existing industry or sectoral regulators on the proposed exercise of powers under new Part 3A**—Senator Keneally invited the Law Council to comment on a proposal of the Business Council of Australia in its submission that there should be a mandatory consultation requirement of this kind, as a pre-condition to the issuance of a ministerial authorisation, or the giving of an action direction or information direction; and

   (5) **parliamentary oversight of the expanded SOCI regime**—Senator Keneally sought the Law Council's views on whether the Committee should have an ongoing oversight role to monitor the operation of the SOCI Act, potentially in addition to a statutory function to periodically review the Act in entirety (by renewing and expanding existing section 60A).

Additional submissions on proposed intervention powers

4. The Law Council also provides some further observations on certain aspects of the intervention powers in proposed Part 3A of the SOCI Act, namely:

   - the importance of external approval of requests for authorisations to exercise governmental intervention powers, in preference to an authorisation regime that is purely internal to the executive government (as is proposed in new Part 3A via a ministerial authorisation regime); and
   - the breadth of powers conferred on the Secretary of the Department of Home Affairs to issue 'information directions' and 'action directions' pursuant to a ministerial authorisation given under new Part 3A. These directions can be issued in respect of a specified 'critical infrastructure sector asset' (being any asset that 'relates to' one of the 11 prescribed critical infrastructure sectors) and not merely the particular asset or assets which have been determined to be a 'critical infrastructure asset' and have been affected by the cyber security incident to which the ministerial authorisation relates.

5. These matters are material to the Law Council's overriding policy objective, to ensure that expansion of the SOCI Act entrenches the core principles of necessity proportionality, transparency, clarity, certainty and efficiency into the legislative framework itself.[1]

Technical issues concerning new Part 3A

6. At the public hearing on 11 June, Law Council witnesses noted certain matters of detail in relation to provisions of proposed Part 3A of the SOCI Act, which are additional to those raised in its primary submission.[2] The following information is provided to supplement those observations.

Notification requirements to regulated entities

7. The Law Council's primary submission recommended that, when ASD exercises powers of intervention pursuant to a Ministerial authorisation and intervention request issued under new Part 3A, it should be subject to analogous notification requirements to those applying to police executing search warrants whenever it removes a computer or device from private premises under proposed section 35BD.

8. In particular, in recommendation 21 and paragraph [173] of the primary submission, the Law Council supported a statutory requirement for ASD to give the regulated entity a written inventory of all computers or devices removed from the premises.

9. To supplement this obligation, the Law Council also supports a further requirement for ASD to provide the regulated entity with formal, official notification of all acts taken pursuant to an information request under proposed section 35AC that involve modifying or deleting data held on a computer, disconnecting a computer or otherwise altering the functioning of a computer.[3] This would ensure equivalency of disclosure obligations of ASD, where it undertakes activities that interfere with private property rights in computers and associated data, even though a physical computer asset is not removed from premises.

10. The Law Council acknowledges that the Bill presently contains requirements in proposed subsection 35AD(3) for regulated entities to be consulted, where possible

---

[1] See further: S Finch, Law Council of Australia, Proof Committee Hansard, 11 June 2021, 1. (Questioner: Senator J Paterson, Chair.)

[2] D Neal SC, Law Council of Australia, *Proof Committee Hansard*, 11 June 2021, 2-3. (Questioner: Senator J Paterson, Chair.)

[3] See further: ibid, 6-7. (Questioner, the Hon M Dreyfus QC MP.)

in the time available, on proposed Ministerial authorisations that would authorise the issuance of intervention requests.[4] The Law Council also acknowledges that the Bill would require regulated entities to be given copies of ministerial authorisations and intervention requests (or records of oral authorisations or requests).[5]

11. However, consultation on the intended terms of a legal authority before it is issued, and the provision of a copy of the final authority to the regulated entity, is materially different to directly informing the regulated entity of all acts which have, in fact, been carried out in ostensible reliance on that authority. The obligations in the Bill do not provide a legal safeguard which ensures full disclosure to the owner or operator of private property, which has been the subject of intervention powers, of the acts that have been carried out. While it would be open to a regulated entity to conduct a forensic review of its computer networks and systems to assess what has been done (as informed by the above disclosure requirements, as well as their observations of ASD's activities in real time) this does not guarantee that all activities will necessarily be identified and imposes an investigative burden upon the regulated entity which could potentially be substantial.

12. Presently, it appears that the only formal *ex post facto* disclosure requirement in the Bill, in relation to the activities which have been carried out under an intervention request, is contained in proposed section 35BH of the SOCI Act. However, this provision is limited to the provision of reports to the Minister for Home Affairs and the Minister for Defence. There is no apparent requirement to make disclosures directly to the regulated entity whose computers and data have been the subject of interference.

Prohibition on ASD taking offensive cyber action

13. As noted at paragraph [122] of the Law Council's principal submission, the Law Council welcomes the inclusion of proposed paragraph 35AB(9)(b) which provides that a Ministerial authorisation given under new Part 3A cannot lawfully support the issuance of an action direction that would require the regulated entity in relation to an asset to take 'offensive cyber action' against the person who is responsible for the cyber incident.

14. That provision is limited to actions taken by the regulated entities and not ASD. However, as also noted in the above passage of the principal submission, the Law Council similarly welcomes the limitation in proposed subsection 35AB(12) on the power to issue Ministerial authorisations that would allow the making of 'intervention requests' to ASD that would involve ASD directly taking such 'offensive cyber action'.

15. At the public hearing on 11 June, Law Council representatives noted that the interaction between proposed subsections 35AB(9) and 35AB(12) is not immediately clear on the face of each individual provision, and if subsection 35AB(9) were read in isolation, it may give some 'end users' an incorrect impression that the compulsory intervention powers in new Part 3A might enable offensive cyber action to be taken in some form (for example, by ASD in carrying out an intervention request issued by the Secretary of the Department of Home Affairs).[6] Accordingly, as an aid to comprehension, consideration might be given to the inclusion of a

[4] In this regard, it is material that proposed paragraphs 35AB(2)(e) and (f) provide that Ministerial authorisations which approve the issuance of intervention requests must specifically approve the exact terms of the relevant intervention request that can be issued. This means that the consultation obligation in proposed subsection 35AD(3) would require the regulated entity to be informed of the terms of any proposed intervention request.

[5] See especially: proposed subsections 35AE(4)-(8) and subsections 35AY(4)-(5) and (7)-(8). (It should further be noted that the regulated entity may have some visibility of at least some of the acts done by reason of its obligation in proposed subsection 35BB(1) to give ASD such assistance as is reasonably required, upon ASD's request, to enable ASD to fulfil an intervention request.)

[6] D Neal SC, Law Council of Australia, *Proof Committee Hansard*, 11 June 2021, 3 (questioner: Senator J Paterson, Chair).

statutory note to proposed subsection 35AB(9), which cross-refers to the related prohibition in subsection 35A B(12) on ministerial authorisations being used to enable ASD to directly take offensive cyber action.

16. To avoid doubt, this issue is separate and additional to the Law Council's submissions and recommendations dealing with the ability of the intervention powers in new Part 3A of the SOCI Act being capable of concurrent exercise with the separate disruptive powers proposed in the Surveillance Legislation Amendment (Identify and Disrupt Bill) 2020. This is particularly important in the case of the proposed data disruption warrants and associated compulsory assistance orders under the latter Bill, which could be used to compel owners and operators of critical infrastructure assets to perform offensive cyber actions to give effect to a data disruption warrant which targets the person or persons behind a cyber-attack, concurrently with ASD executing an intervention request under the SOCI regime for the purpose of responding to and recovering from that attack.[7]

Limitations in statutory immunities

17. Senator Keneally invited the Law Council to provide, on notice, legislative suggestions to address gaps in the proposed immunities for the personnel of regulated entities under the expanded SOCI regime.[8]

18. The Law Council's key suggestion for legislative improvement is set out in recommendation 34 and paragraphs [339]-[354] of its principal submission.

19. In particular, the Law Council has noted that subsection (2) of proposed sections 35AAB. 35AW, 35BB and 30BE of the SOCI Act are limited to persons who are 'employees, officers or agents' of the regulated entity that is responsible for a critical infrastructure asset. As these expressions are undefined in the Bill and will therefore take their ordinary meanings, the Law Council's considers there is a material risk that they will not adequately cover the diverse range of business models utilised across the 11 sectors proposed to be regulated. For example:

    - the concept of an 'employee' does not appear to cover contractors who provide services to a regulated entity to enable the relevant critical infrastructure asset to function (and whose cooperation may be essential to the regulated entity complying with its new or expanded obligations under the SOCI regime); and
    - the concept of an 'employee', 'officer' or 'agent' of a regulated entity does not clearly cover circumstances in which a regulated entity forms part of a group of related corporations, and the personnel of a related corporation provide services to the regulated entity. It is conceivable that the involvement of the personnel of the related corporation and contractors might be necessary to enable a regulated entity to comply with some of or all its new obligations under the SOCI Act.

20. The Law Council has recommended that a more expansive immunity is applied, which could be modelled on existing provisions of paragraph 70AA(1)(c) of the *Banking Act 1959* (Cth), which already address this issue for the banking and financial services sector with respect to that regulatory regime. This more expansive immunity would help address the need for certainty and cooperation.

[7] Law Council of Australia, Principal Submission, (17 February 2021), 47-48 at [122]-[129] and recommendation 14.

[8] Senator the Hon K Keneally, *Proof Committee Hansard*, 11 June 2021, 4.

Further expansion of SOCI regime to supply chains

21. Senator Fawcett sought the Law Council's views about whether, and if so how, the expanded SOCI regime might be further expanded to comprehensively cover obligations with respect to supply chain resilience in each regulated sector.[9]

22. The Law Council notes that the regulatory framework proposed in the Bill appears to be capable of covering at least some supply chains in relation to various assets within the 11 'critical infrastructure sectors' proposed to be regulated. This primarily reflects three circumstances. First, some of the regulated sectors may, themselves, form part of supply chains to other regulated sectors. For example:

    - the data storage or processing and communications sectors (as proposed to be defined in section 5 of the SOCI Act, per item 7 of Schedule 1 to the Bill) will, almost invariably, provide services to entities within the other regulated sectors under the expanded regime; and
    - the 'health care and medical sector' is proposed to be defined in section 5 of the SOCI Act (per item 7 of Schedule 1 to the Bill) as including a sector of the economy that involves the provision of 'health care' (defined to include a range of services, including pharmacy and numerous fields of allied health) and the production, distribution or supply of 'medical supplies' (defined to cover goods for therapeutic use and other things specified in statutory rules). This would appear to make it possible for suppliers of goods and services to hospitals and other primary health care service provides to be covered by the expanded SOCI regime.

23. Secondly, the expanded obligations sought to be imposed on the responsible entities for regulated assets may require those responsible entities to take steps to identify hazards or risks in their respective supply chains, and manage them to the greatest extent possible (for example, through their selection of suppliers and the completion of due diligence in relation to cyber or physical security arrangements).

24. For instance, the obligations under new Part 2A of the SOCI Act (especially those in proposed section 30AH) for the responsible entities for critical infrastructure assets to adopt and comply with risk management programs require those plans to identify each hazard which may have a material risk of having a 'relevant impact' on the asset, and minimise or eliminate that risk so far as possible. The definition of a 'relevant impact' in proposed section 8G covers both direct and indirect impacts on the availability, integrity or reliability of the critical infrastructure asset, or information (including data) that is stored in, or is about, the asset. The inclusion of indirect impacts may be capable of covering hazards arising from failures in the supply chain to a particular critical infrastructure asset. However, the extent to which proposed Part 2A may operate to impose obligations with respect to supply chains may depend on the content of statutory rules made under that Part, should the Bill pass.

25. Thirdly, some of the specific powers and associated obligations in the Bill explicitly recognise interdependencies (which could include the circumstances in which a particular asset forms part of a supply chain to another critical infrastructure asset). For example:

    - proposed section 52B provides that the Minister for Home Affairs is required to consider various matters in deciding whether to make a declaration that a particular critical infrastructure asset is a 'system of national significance' (and therefore subject to enhanced cyber security obligations in proposed Part 2C). Proposed paragraph 52B(2)(b) requires the Minister to consider the nature

[9] Senator D Fawcett, *Proof Committee Hansard*, 11 June 2021, 6.

and extent of any interdependencies (to the extent known) between the asset and any other critical infrastructure assets; and

- the Ministerial authorisation-based intervention regime in proposed Part 3A, and specifically in proposed section 35AB:
  - is enlivened by the existence of a cyber security incident that has had, is having, or is likely to have, a 'relevant impact' on a critical infrastructure asset (known as the 'primary asset' for the purpose of that Part). In applying the concept of a 'relevant impact' as defined in proposed section 8G (summarised above) the intervention regime may be capable of covering cyber security incidents that have an indirect impact, because of disruptions to a supply chain; and
  - enables the issuance of 'information directions', 'action directions' and 'intervention requests' that 'relate to' the cyber security incident and a 'specified critical infrastructure sector asset'. The latter term, as defined in proposed subsection 8E(1), covers any asset that 'relates to a critical infrastructure asset'. This could therefore cover assets in the supply chain.

26. If there is a concern that, despite the above measures, the expanded regulatory regime proposed in the Bill does not comprehensively cover supply chains in relation to critical infrastructure assets that are regulated, the Law Council submits that this issue ought to be examined as part of a separate review and possible law reform process. This course of action would recognise the potentially significant regulatory impost of an even further expansion of the obligations proposed in the Bill, and further overlap with other regulatory regimes that regulate the various parties in the supply many of which are in different and discrete sectors of the economy. It would provide a dedicated forum to thoroughly scrutinise their implications in consultation with key stakeholders (including civil society as well as industry) and avoid unintended consequences.

27. In particular, the Law Council cautions that any implications for foreign investment laws should be given careful consideration, especially taking account of the issues raised at paragraphs [68]-[76] and recommendation 8 of the Law Council's principal submission.

Consultation requirements

28. Senator Keneally sought the Law Council's views on the following recommendation of the Business Council of Australia (**BCA**):

> *Many of the proposed sectors are already highly regulated, including on the price of services offered to consumers or on maximum revenue (such as for the energy network). This means that additional compliance costs from the SOCI Act (which would generally have to be passed on as costs for all consumers) will instead have to come from foregone investment or reduced efficiency and competition as it becomes increasingly unattractive for operators to participate in the market.*
>
> *Existing regulators should be consulted on relevant decisions made under the SOCI Act to ensure they can consider potentially substantial regulatory compliance costs in making determinations relevant to their sector.*[10]

29. In the alternative, the BCA supported a further statutory precondition to the exercise by the Minister for Home Affairs of the power in proposed section 52B of the SOCI Act (item 66 of Schedule 1 to the Bill) to make a declaration designating a critical

[10] Business Council of Australia, Supplementary Submission 75.1, 11 June 2021, 4.

infrastructure asset as a ‘system of national significance’. This alternative proposal would explicitly require the Minister to consider the effects that the designation may have on 'the efficiency of and competition in the relevant sector'.[11]

30. The Law Council is supportive, in principle, of these proposals. They would facilitate one of the core policy objectives identified by the Law Council that the expanded SOCI regime should deliver regulatory certainty, including in relation to its interaction with existing regulatory regimes applicable to critical infrastructure sectors. This objective is not limited to the avoiding duplication or conflict between the SOCI regime and existing sectoral regulations, but also to preventing unintended regulatory consequences.

31. For example, there is at least a theoretical possibility that compliance costs or other limitations arising from the expanded obligations under the SOCI regime may have downstream impacts on regulatory pricing determinations, such as those made by the Australian Energy Regulator under the *Competition and Consumer Act 2010* (Cth) (and relevant State and Territory laws) in relation to the wholesale and retail energy markets, and energy networks.

32. Similarly, the Law Council also emphasises the evidence of its representatives at the public hearing on 11 June, about the potential for conflict between directors’ duties under the *Corporations Act 2001* (Cth) and expanded obligations under the SOCI regime; together with obligations under the regulatory regime for prudential standards for the banking, insurance and superannuation industries.[12] The Law Council considers that these areas of regulation could potentially raise some of the most significant and complex interaction issues with the expanded SOCI regime.

33. The Law Council acknowledges that the extrinsic materials to the Bill convey a policy intention to avoid, to the greatest possible extent, regulatory duplication or inconsistency. This includes via the adoption of a ‘co-design’ process for the development of statutory rules and other legislative instruments under the SOCI Act in anticipation of the passage of the Bill.[13] It would also be open to the Minister for Home Affairs to exercise a general discretion to consult with relevant sectoral regulators before making a determination that a ‘critical infrastructure asset’ is a ‘system of national significance’ under proposed section 52B, or prior to making any other administrative decisions under the expanded SOCI Act. It would further be open to the Minister for Home Affairs under proposed section 49A of the SOCI Act (per item 57 of Schedule 1 to the Bill) to designate an existing sectoral regulatory body as a ‘relevant Commonwealth regulator’ for the purpose of exercising investigation, monitoring and enforcement powers under the SOCI Act.

34. However, all of these measures rely solely on executive discretion about whether and how existing sectoral regulators are engaged, for the purpose of identifying and managing or avoiding regulatory duplication or conflict. There is no express acknowledgement or supporting requirements which provide that measures taken to comply with existing industry specific requirements will routinely and consistently be taken to comply with the SOCI regime. The inclusion in the SOCI Act of explicit statutory requirements for consultation with applicable sectoral regulatory bodies for this purpose—as a legal pre-condition to the exercise of powers or performance of functions under the SOCI Act—could provide a stronger degree of assurance to regulated entities (and sectoral regulators) that such consultation will occur, and

[11] Ibid, 4 and 5 (rec 6).

[12] S Finch, Law Council of Australia, *Proof Committee Hansard*, 11 June, 4. (Questioner: Senator the Hon K Keneally).

[13] See, for example: Explanatory Memorandum, Attachment B at [4.2.1] (costs of critical infrastructure risk management programs), [4.2.2] (costs of enhanced cyber security obligations), [4.2.3] (costs of enhanced government assistance), and [5.2] (key findings from industry consultations, including that ‘co-design and implementation are key’ and recognition of the importance of ‘leveraging existing regimes and reducing regulatory impost’) (pages unnumbered).

outcomes of the consultation process appropriately addressed. Similarly, where SOCI requirements overlap with existing regimes addressing cyber security and related matters[14] or address complementary obligations, the SOCI regime would benefit by addressing expressly such existing or overlapping requirements by adding provisions that make it clear that compliance with such requirements can be and are to be taken to meet and address the SOCI requirements and can operate by means of a 'safe harbour' by addressing compliance and serving as evidence of such compliance. The Law Council observes that a statutory consultation requirement of general application and a form of express recognition of existing obligations could facilitate a consistent, orderly, efficient, and transparent process for such consultations to occur.

35. The Law Council also observes that the policy objectives of the BCA, in making the recommendation outlined above, also appear broadly consistent with the basis for the Law Council's recommendation 1, to strengthen various statutory consultation pre-conditions to the making of Ministerial rules under the expanded SOCI regime.[15]

Parliamentary oversight functions

36. Senator Keneally asked whether the Law Council would support the Committee having an oversight role in monitoring the exercise of the new powers under the expanded SOCI regime, particularly the intervention powers under new Part 3A. This might include, for example mandatory notification and briefing requirements when those powers are exercised.[16]

37. The Law Council is supportive of the Committee having an ongoing monitoring function in relation to the performance of functions and exercise of powers under the SOCI Act, in addition to performing a periodic statutory review of the operation of the Act in entirety. Section 60A of the SOCI Act presently provides for a review of the latter kind on a 'one-off' basis, and the Law Council's recommendation 31 suggests that this should be amended to require a periodic review of the SOCI Act every three years. The conferral of an additional ongoing monitoring function upon the Committee (which has the ability to receive classified or otherwise confidential information in camera) would also supplement the annual reporting requirements proposed in the Bill.

38. The Law Council considers that it would be sensible and prudent for the Parliament, via the Committee, to receive timely briefing on the exercise of the extraordinary powers in Part 3A of the SOCI Act, so that it has visibility and understanding of the manner and context in which they are used, and has working knowledge of the internal systems, processes and administrative arrangements in place to support the exercise of those powers.

39. It is desirable that such Parliamentary briefings occur in as close proximity as is reasonably practicable to the relevant cyber security incident, rather than this potentially occurring belatedly in the context of a periodic (three-yearly) review by the Committee of the SOCI Act in its entirety. The timely provision of such briefings could equip the Committee with important contextual information for its subsequent periodic reviews. More broadly, this may aid its oversight and scrutiny of other national security legislation which operates alongside the SOCI Act.

---

[14] See, for example, Australian Prudential Regulatory Authority, *Prudential Standard 234: Information Security*, (July 2019) <https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf>. (**Prudential Standard CPS 234**). The object of this standard is to 'ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyberattacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats': at 1.

[15] Law Council, Primary Submission, (17 February 2021), 23-26 at [14]-[32].

[16] Senator the Hon K Keneally, *Proof Committee Hansard,* 11 June 2021, 8.

40. Significantly, section 29 of the *Intelligence Services Act 2001* (Cth) (**ISA**) already contains considerable precedent for the Committee to have an ongoing monitoring role over various national security powers of an extraordinary nature. For example, paragraphs 29(1)(baa) and (bba) give the Committee an ongoing monitoring role in relation to the counter-terrorism powers of the Australian Federal Police under Part 5.3 of the *Criminal Code Act 1995* (Cth) and Division 3A of Part IAA of the *Crimes Act 1914* (Cth). In addition, paragraph (c) of subsections 9B(8A) and 9C(6) of the ISA provide a mechanism for the Committee to be informed of emergency authorisations issued under Part 2 of that Act to enable the urgent collection of certain intelligence outside Australia.

41. The Law Council acknowledges that the Committee has a general power in section 30 of the ISA to request briefing from various agency heads, including the Secretary of the Department of Home Affairs and the Director-General of ASD. However, this power is expressed as being exercisable for the specific purpose of the Committee performing its functions in section 29 of the ISA. As section 29 does not presently confer specific functions on the Committee in relation to the SOCI Act, there may not be a clear and certain basis for comprehensive briefing on this matter.

42. The enactment of a specific provision empowering the Committee to perform an ongoing monitoring role in relation to the SOCI Act, or at least the intervention powers in proposed Part 3A, would provide clarity and certainty about the nature and extent of Parliamentary visibility over these extraordinary powers. Importantly, it would clearly convey, in advance, Parliament's expectation about the visibility it should have over those matters.

Additional submissions on proposed Part 3A powers

43. The following submissions address two further issues relevant to proposed Part 3A of the SOCI Act, which complement the matters raised in the Law Council's primary written submission and oral evidence to the Committee.

Importance of an external, independent approval mechanism

44. In paragraphs [108]-[113] and recommendation 12 of its primary submission, the Law Council recommended that the proposed Ministerial authorisation regime in new Part 3A should be replaced with an external authorisation mechanism. The Law Council suggested that this independent approval mechanism could be analogous to that recommended by the third Independent National Security Legislation Monitor (**INSLM**) for the extraordinary powers in Part 14 of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) to compel private communications providers to render specified technical assistance to law enforcement agencies. (That model would involve the creation of a specialist division of the Administrative Appeals Tribunal, headed by a retired judge.)

45. In discussing the Law Council's proposal for external authorisation at the hearing on 11 June, some Committee members commented on the following analogy, as described by the Chair:

> ***CHAIR**: …in relation to the ASD step-in powers, in the event of a crisis, it's quite likely that extremely rapid action will be necessary to address this. It's a crude analogy, but it's been put to me that when a building is on fire and the fire brigade turns up you don't debate with the fire brigade whether it's necessary to turn on the hoses and start putting out the fire and have a discussion about what the consequences of that were. In some of these instances, are we really going to have time to*

litigate with the ASD about whether it's necessary for it to jump on the system and defeat an attacker or protect a system?[17]

46. The following consolidation of the key points made in the Law Council's oral evidence and primary written submission may assist the Committee's consideration of whether such an analogy ought to apply to the proposed intervention powers:

- the proposed intervention powers in the Bill could potentially operate in relation to an incident that occurs over a protracted period of time (for example, in the range of months) rather than the typically shorter duration of a physical hazard requiring an emergency response, such as a fire to a structure.[18] (This is reflected in proposed section 35AG, which provides that ministerial authorisations have a maximum duration 20 days, with an explicit ability for an unlimited number of fresh ministerial authorisations to be given in the same terms as an expired authorisation);
- the nature of compulsory governmental intervention in a response to a cyber security incident affecting a privately owned critical infrastructure asset is likely to require a sophisticated understanding of the impacts (both direct and indirect, and immediate and latent) of the proposed intervention activities on the relevant business. This is not necessarily the case for a physical hazard requiring an immediate emergency response, such as a structural fire.[19] The regulatory impact statement appended to the Explanatory Memorandum to the Bill acknowledges there is a risk that Governmental intervention may lead to 'adverse, unintended consequences which may occur as a result of Government not understanding a critical infrastructure asset's control systems'.[20] However, the Law Council considers that this risk is not given sufficient recognition or treatment in the proposed legislative framework, and that disproportionate reliance is placed on *ad hoc* consultation. This could be improved significantly by an independent authorisation mechanism for intervention powers;
- the intervention power in proposed Part 3A of the SOCI Act shares many common features with the compulsory industry assistance powers in Part 14 of the Telecommunications Act, which led to the third INSLM recommending a model of independent authorisation for the latter powers. In particular, the third INSLM placed determinative weight on the extraordinary powers of coercion able to be exercised against private service providers, the gravity of those powers, and the need for the highest levels of public trust and confidence in that regime. The third INSLM specifically commented that reliance on the involvement of multiple Ministers in an internal authorisation process did not create a sufficient degree of rigour and independence;[21] and
- many warrant-based authorisation regimes make provision for the applicant and issuance of warrants (by an external issuing authority) on an urgent basis, including via oral means (including by telephone) rather than in writing. This includes search warrants, telecommunications interception warrants and surveillance device warrants.[22] This circumstance tends in support of a conclusion that an external authorisation model can be feasible, even in circumstances of significant urgency. Similarly, there is ample precedent in the context of civil enforcement and private legal proceedings, including the ability to obtain urgent *ex parte* orders in the nature of injunctions and asset

[17] Senator J Paterson, Chair, *Proof Committee Hansard*, 11 June 2021, 3.

[18] S Finch, Law Council of Australia, *Proof Committee Hansard*, 11 June 2021, 4. (Questioner: Senator the Hon K Keneally).

[19] Ibid.

[20] Explanatory Memorandum, Attachment B (regulatory impact statement), [4.2.3] (costs of Government assistance) (pages unnumbered).

[21] Law Council, Principal Submission, 17 February 2021, 45 at [110].

[22] See further: D Neal SC, Law Council of Australia, *Proof Committee Hansard*, 11 June 2021, 3.

freezing orders, variously under the common law and numerous statutory regulatory regimes.

Breadth of information and action direction powers

47. The Law Council wishes to draw the Committee's attention to the broad scope of the 'information direction' powers under proposed section 35AC of the SOCI Act. The Ministerial authorisation regime in new Part 3A would enable the issuance of 'information directions' and 'action directions' to the responsible entities for 'critical infrastructure sector assets' (as defined in proposed section 8E) as well as the responsible entities for 'critical infrastructure assets' (as defined in section 9, which is proposed to be expanded by Bill). This means that the entities which can be compelled to provide information include the owners and operators of assets that in some way 'relate to' a critical infrastructure sector, not only the assets that have been specifically determined to be 'critical infrastructure assets' for the purpose of the expanded SOCI regime.

48. The Law Council acknowledges the expression of policy intent in the Explanatory Memorandum to ensure that the powers are available to deal with interdependencies between critical infrastructure assets, and other assets (such as those in supply chains).[23] The Law Council does not categorically oppose the ability to compel the provision of relevant information from entities other than those who are responsible for the primary asset affected by the cyber security incident. However, the power should only be available in such circumstances where it is demonstrably necessary and proportionate.

49. In this regard, the breadth of the information direction power underscores the importance of implementing several of the Law Council's recommendations numbered 12-37, which are directed to giving comprehensive assurance to all regulated entities (particularly in the form of commensurately broad immunities from legal liability), and facilitating clarity, certainty, transparency, and proportionality in the operation of the expanded regime.

Reporting of incidents and other matters

50. At the public hearing on 11 June, Law Council representatives[24] noted that some requirements were very broad and could not be consistory applied in practice, for example some of the reporting provisions in Part 2B of the Bill as they apply to cyber security incidents.[25] Much of the difficulty stems from a lack of objective criteria as to materiality regarding the concept of a hazard as used in the Bill. For example, the term 'hazard' is used in the definition of 'relevant impact' in proposed section 8G with no reference back the degree of the hazard in question. Similarly, the definition of a 'cyber security incident'[26] does not depend on a test of materiality. The Law Council notes that such difficulties can go to the core of the regime, as reporting obligations will apply to many organisations in various sectors and form part of respective their daily compliance and governance requirements. As noted above, this includes organisations in the supply chain for the provision of goods and services to many other organisations in various sectors of the economy. Clarity and certainty are therefore key to the successful operation of the regime on a national, economy wide scale.

[23] Explanatory Memorandum at [884]-[885] (pages unnumbered).

[24] O Ganopolsky, Law Council of Australia, *Proof Committee Hansard*, 11 June 2021, 4. (Questioner: Senator the Hon K Keneally).

[25] For example, proposed sections 30BC and 30BD.

[26] Proposed section 12M.

51. The Law Council notes that the Bill would add three additional objects to the SOCI Act.[27] These objects refer to providing a regime that address cybersecurity incidents that are 'serious',[28] and the imposition of enhanced obligations on 'systems of national significance'.[29] The Law Council makes the following recommendations, which supplement recommendations 9 and 10 in its principal submission:[30]

    (a) a materiality test be added to assessment of availability, integrity, reliability, or confidentiality of the given critical infrastructure asset. The Law Council notes that the Explanatory Memorandum refers to matters such as 'critical' cyber security incident, [31] by contrast to other provisions that apply 'irrespective of the significance'.[32] The test of materiality can reflect the diverse nature of matters that impact on security by listing relevant matters that are to be considered based on the nature of the risk to be addressed. This can be aligned to existing obligations and reporting thresholds applicable to relevant breaches, industries or types of infrastructure or types of harms to be addressed. The notifiable data breach regime under the *Privacy Act 1988* (Cth)[33] and reporting requirements for information security incidents under APRA prudential standard CPS 234[34] can provide relevant examples. Consideration could also be given to articulating materiality by reference to impacts that are immediate and may be 'minimal' compared to impacts on 'essential' services as noted in the Explanatory Memorandum;[35]

    (b) express provisions be added to address how notification under one (existing) regime can be said to comply with reporting and notification under the Bill; and

    (c) a test of materiality be added to address how the asset could be said to impact on matters of 'national' significance. The Law Council appreciates that matters of national significance or security can traverse a broad cross section of risks and matters. The scope and variety of matters can be addressed by a list of factors to be considered and used to inform the risk assessment process undertaken by regulated assets and their respective owners, the rule making process and notifications under the Bill.

[27] Proposed paragraphs 3(c), (d) and (e)

[28] Proposed paragraph 3(e).

[29] Proposed paragraph 3(d).

[30] Law Council of Australia, *Principal Submission*, (17 February 2021), 36-40 at [77]-[90].

[31] Explanatory Memorandum, [317] (pages unnumbered).

[32] Ibid, [322] (pages unnumbered).

[33] *Privacy Act 1988* (Cth), Part 3C and definition of an 'eligible data breach' in sections 26WE and 26WF.

[34] APRA, *Prudential Standard CPS 234: information security*, (July 2019), Clause 35(a).

[35] Explanatory Memorandum, [323] (pages unnumbered).