Law Council
OF AUSTRALIA

Office of the President

6 April 2023

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

Dear Secretary

Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023

1. The Law Council is grateful for the opportunity to respond to the Parliamentary Joint Committee on Intelligence and Security's (the **Committee's**) review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023 (the **Bill**).

2. The Law Council has been unable to consider all aspects of the Bill in detail because of the limited time for consultation, nor has it had the opportunity to adequately consult with its membership on the proposed reforms. For this reason, the views expressed in this submission are preliminary and the Law Council has only responded to select issues. For the avoidance of doubt, the absence of specific comment in relation to a provision should not be read as an implicit endorsement of that provision by the Law Council.

3. The Law Council has extensively considered the principles underpinning the legislative framework and operations of the National Intelligence Community (the **NIC**) in its response to the Comprehensive Review of the Legal Framework Governing the National Intelligence Community (the **Richardson Review**).[1]

4. In principle, the Law Council recognises that NIC agencies must be well-equipped to face national security threats and that the Australian Government has a primary responsibility to protect the life and security of the person. However, in order to preserve the values that underpin our democratic society, Australia's laws must be reasonable, necessary and proportionate to achieve a legitimate objective.

5. The Law Council notes the constructive role it has played—with the advantage of an adequate period for consultation—in previous iterations of law reform to implement recommendations made by the Richardson Review. In particular, the Committee

[1] See more generally, the Law Council's submission to the Richardson Review: Law Council of Australia, Submission to Dennis Richardson AO Attorney-General's Department, Comprehensive review of the legal framework governing the National Intelligence Community (27 November 2018) 9-10. ('***LCA 2018 Richardson Review Sub***')

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

considered favourably[2] the Law Council's targeted proposals for improvement in relation to the Committee's Review of the National Security Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021.[3]

Proposed extension of defences for certain national infrastructure related offences

6. Part 2 of Schedule 1 to the Bill proposes new immunities from criminal liability for Australian Security Intelligence Organisation (**ASIO**) officers:

- **Item 6**—would establish a new defence for ASIO officers, applying to offences against subsections 474.6(1) and (3),[4] which are offences pertaining to interference with telecommunications facilities, if the ASIO officers are acting in good faith in the course of their duties (in the case of ASIO affiliates, this would include where they are acting in accordance with their contract, agreement or other arrangement) and their conduct is reasonable in the circumstances for the purpose of performing that duty;
- **Item 8**—would establish a new defence for ASIO officers for offences under subsection 477.2(1) if the ASIO officers are acting in good faith in the course of their duties (in the case of ASIO affiliates, this would include where they are acting in accordance with their contract, agreement or other arrangement) and their conduct is reasonable in the circumstances for the purpose of performing that duty.
- Both new defences define 'ASIO officer' broadly to mean:
  - the Director-General of Security; or
  - an 'ASIO employee' (within the meaning as in the *Australian Security Intelligence Organisation Act 1979*); or
  - an 'ASIO affiliate' (within the meaning of that act).

7. It is relevant to note that ASIO, along with law enforcement agencies, already has defences to offences involving interference with facilities and the modification of a telecommunications device identifier offence.[5]

8. The Explanatory Memorandum states that these defences are required because ASIO officers are constrained in how they can accurately identify the location of a device 'due to concerns that more efficient methods would risk liability for offences under Parts 10.6 and 10.7 of the Criminal Code'.[6]

9. The Law Council acknowledges the Richardson Review considered the introduction of offence specific immunities a 'reasonable and pragmatic solution' to the interaction of

[2] Parliamentary Joint Committee on Intelligence and Security, Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018 (September 2021) 3.62 -3.63.
[3] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021 (1 February 2022). ('***LCA Comprehensive Review, 1 February 2022 Submission***')
[4] Subsection 474.6(1) provides that a person commits an offence if the person tampers with, or interferes with, a facility owned or operated by a carrier, a carriage service provider or a nominated carrier. Subsection 474.6(3) provides that a person commits an offence if a person tampers or interferes with a facility owned or operated by a carrier, a carriage service provider or a nominated carrier, and this conduct results in hindering the normal operation of a carriage service supplied by a carriage service provider.
[5] For example, Subsection 474.6(5) makes it an offence for a person to use or operate any apparatus or device which hinders the normal operation of a carriage service. Subsection 474.6(7) provides a defence for a law enforcement officer, or an intelligence or security officer, acting in good faith in the course of his or her duties where the conduct of the person is reasonable in the circumstances for the purpose of performing that duty.
[6] Explanatory Memorandum, 18 [41]

new geolocation technologies with telecommunications offences that pre-date these challenges.[7] Relevantly, the ASIO submission to the Committee notes:

> *Identifying and locating subjects of interest is a core part of this role. A person's digital footprint—for example which devices they are using and where those devices are located—provides key enabling information.*[8]

10. In relation to analogous criminal immunities for computer-related acts in Division 476 of the Criminal Code, the Law Council did not oppose extending criminal immunities in favour of the Australian Signals Directorate (**ASD**) as part of the inquiry into the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**SOCI Bill**) and also in relation to the proposed expansion of the criminal immunity to Australian Secret Intelligence Service (**ASIS**) and Australian Geospatial-Intelligence Organisation staff members.[9]

11. However, the Law Council notes the caution expressed by the Richardson Review that these targeted defences be used in a necessary and proportionate manner and the importance of considering unintended adverse impacts:

> *When ASIO is acting without a warrant, ASIO must carefully consider whether the use of these techniques in the circumstances is necessary, proportionate, reasonable and justified. Simply because the techniques will be more efficient does not mean it is the best method to use in every set of circumstances. The Review considers that ASIO must avoid adverse impacts that could arise—for example, it would not be reasonable to use methods that prevented a person from making Triple Zero, emergency or distress calls or which resulted in* network failure.[10]

12. The Explanatory Memorandum provides little guidance on how the expanded immunities may impact on the warrant and issuing safeguards regarding interceptions and access to telecommunications and data under the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**). The Committee agreed with the Law Council on the importance of this consideration in the context of its Advisory Report on the SOCI Bill and Statutory Review of the Security of Critical Infrastructure Act 2018.[11]

13. The Explanatory Memorandum places critical weight on the safeguards afforded by compliance with the 2020 Minister's Guidelines to ASIO (the **Minister's 2020 Guidelines**). Relevantly, the Explanatory Memorandum states:

> *All activities will be conducted in line with the guidelines issued by the Minister for Home Affairs, which require ASIO to only undertake activities which are proportionate, and using the least intrusive method available.*

14. The Law Council has extensively considered the Minister's 2020 Guidelines.[12] While the Law Council noted these Guidelines made several important improvements to the 2007 Guidelines, several important matters remain unaddressed. In summary, the

---

[7] Commonwealth of Australia, Attorney-General's Department, Comprehensive Review of the Legal Framework of the National Intelligence Community (December 2019), vol. 2, 190-191 [24.63]. ('***Richardson Review***')
[8] Australian Security Intelligence Organisation, ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security (April 2023) 2.
[9] LCA Comprehensive Review, 1 February 2022 Submission, 50-51.
[10] Richardson Review, vol. 2, 191 [24.67]
[11] Parliamentary Joint Committee on Intelligence and Security, Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018 (September 2021) 49 [3.62].
[12] Law Council of Australia, Comments on the Minister's Guidelines to the Australian Security Intelligence Organisation (13 August 2020). ('***LCA Comment on Minister's Guidelines to ASIO***')

Law Council remains concerned that the Minister's 2020 Guidelines provide insufficiently precise and clear guidance in the following respects:[13]

- **categories of particularly sensitive information**—specific guidance on the collection, use, disclosure, storage, destruction or retention of categories of particularly sensitive information, such as:
  - information that is, or is likely to be, subject to client legal privilege or parliamentary privilege;
  - health information (such as medical records) and biometric information (such as fingerprints); and
  - journalistic information, such as the identity of journalists' sources, and the information provided by those sources;
- **bulk personal data**—specific guidance on the acquisition, interrogation, retention and destruction of bulk personal datasets;
- **targeting vulnerable persons**—guidance on exercising coercive or otherwise intrusive intelligence collection powers against vulnerable persons, including children, people with disabilities, and people who belong to minority groups.

15. The Law Council reiterates its recommendation that the Minister's 2020 Guidelines should be revised and re-issued, tabled in Parliament, and reviewed by the Committee.

Definition of ASIO Officer

16. The proposed definition of 'ASIO Officer' is expressed broadly and goes beyond the scope of the recommendations of the Richardson Review. As indicated above, the definition of 'ASIO Officer' includes an 'ASIO Affiliate', which is defined by the *Australian Security Intelligence Organisation Act 1979* (Cth) to mean 'a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement, and includes a person engaged under section 85 and a person performing services under an agreement under section 87'.[14]

17. The Law Council submits that the relevant sections of the Richardson Review do not discuss the extension of these immunities to ASIO affiliates.[15] The Law Council remains concerned that there is the potential for 'ASIO Affiliate' to allow other officers of law enforcement agencies, such as the AFP, or other intelligence agencies with an offshore intelligence focus, such as ASIS, to rely on the defence. This is undesirable. It would carry the risk of undermining the differentiated warrant and issuing safeguards—for example, the issuing safeguards regulating access to telecommunications data and interceptions under the TIA Act. The Law Council's long-standing position is that the vital distinction between foreign and security intelligence should be maintained.

Amendment to Ministerial authorisations

18. Part 9 of Schedule 1 to the Bill seeks to amend the *Intelligence Services Act 2001* (Cth) (the **IS Act**) to provide certainty regarding the level of detail required to describe the directed activities (which can be of a specific or general nature, or by way of a class or classes) in a ministerial direction under paragraph 6(1)(e).

[13] LCA Comment on Minister's Guideline to ASIO, 6-7 [9].
[14] Section 4, *Australian Security Intelligence Organisation Act 1979 (Cth).*
[15] Richardson Review, vol 2, 188-191.

19. The Law Council is concerned that this aspect of the Bill goes beyond the scope of the recommendations in the Richardson Review, fails to achieve certainty, and may have the unintended consequence of entrenching a deficient standard of detail in ministerial directions. These issues are discussed below.

20. The Law Council is not satisfied by the quality of the justification provided by the Explanatory Memorandum. In essence, the justification for these consequential amendments consists of two paragraphs in the Explanatory Memorandum.[16] The human rights implications of these proposed amendments are also not adequately explained in the statement of compatibility. The Law Council recommends that these issues be more fully explored in a Supplementary Explanatory Memorandum, or, alternatively, that Part 9 of Schedule 1 be split into a separate Bill and be considered separately with adequate time periods for consultation.

21. The Explanatory Memorandum identifies that the purpose of these amendments is to streamline existing practice:

> *The practice to date has been for the Minister to direct ASIS to undertake activities predominantly by reference to a purpose. Review and consideration of the provision has identified the need for greater certainty about the level of detail required to specify activities in a direction.*[17]

22. The Explanatory Memorandum suggests the following examples of possible streamlined ministerial directions that might be enabled by the amendments, directions to:

- interfere in the movement of an individual outside Australia suspected of involvement in a terrorist attack;
- disrupt the supply of weapons to terrorist organisations outside Australia;
- degrade the capabilities of terrorist organisations outside Australia; or
- communicate information for the purpose of disrupting terrorism outside Australia.[18]

23. Crucially, the Explanatory Memorandum states that 'where a class (of intelligence activities) has been specified by the Minister, ASIS will be responsible for satisfying itself that a proposed activity falls within the specified class'.[19] The Law Council is concerned that Part 9 of Schedule 1 to the Bill leaves an impermissibly wide ambit of discretion for ASIS. This carries the risk of undermining the primacy of ministerial responsibility and accountability as a key underpinning of the authorisation mechanism in Part 2 of the IS Act. Any ability for agency heads to give internal authorisation should be regarded as an exceptional measure.

24. The Law Council notes that the suggested amendments in Part 9 of Schedule 1 to the Bill do not correspond with any of the recommendations made in the Richardson Review. However, the Richardson Review noted that the requirement to seek ministerial authorisation for activities resulting in a direct effect under its 'other activities' function was included in the Act to implement a recommendation of the Joint Select Committee on Intelligence Services.

[16] Explanatory Memorandum, 32 [153] and [154].
[17] Explanatory Memorandum, 32 [153].
[18] Explanatory Memorandum, 32 [154].
[19] Ibid, 32 [153].

25. In this regard, the Richardson Review cited the following passage from the Joint Select Committee on Intelligence Services:

> *in cases where the responsible Minister may activate 'other activities' under 6(1)(e) which relate to Australian citizens or Australian organisations overseas, then further accountability is required. This can be achieved through connecting the operation of 6(1)(e) to clauses 8 and 9 of the IS Act which provide for Ministerial directions and authorisations.*[20]

26. That close connection between the operation of sub-paragraph 6(1)(e) with the related statutory pre-conditions directed to establishing necessity and proportionality is summarised briefly below.

27. Subsection 6(1) of the IS Act prescribes the functions of ASIS, paragraph 6(1)(e) provides the broadest function in the following terms:

> *to undertake such other activities as the responsible Minister directs relating to the capabilities, intentions or activities of people or organisations outside Australia.*[21]

28. The responsible Minister, in reliance of paragraph 6(1)(e), may make a direction only if the Minister:

- has consulted other Ministers who have related responsibilities; and
- is satisfied that there are satisfactory arrangements in place to ensure that, in carrying out the direction, nothing will be done beyond what is necessary having regard to the purposes for which the direction is given; and
- is satisfied that there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in carrying out the direction will be reasonable having regard to the purposes for which the direction is given.[22]

29. Sub-paragraph 8(1)(a)(ii) provides the Ministerial Direction must require the agency to obtain an authorisation under section 9, 9A or 9B of the IS Act[23] before undertaking, in accordance with a direction under paragraph 6(1)(e), an activity, or a series of activities, that will, or is likely to, have a 'direct effect on an Australian person.'

30. The Law Council has previously described the dual-function of the authorisation safeguards, and in particular section 9, 9A or 9B of the IS Act, contained in Part 2 of the IS Act in the sense of:

- **condition precedent to all intelligence collection on an Australian person**: failure to comply with a requirement to obtain a statutory authorisation—even if the relevant actions through which intelligence was produced are not otherwise unlawful—may invalidate the agency's purported performance of its functions in collecting intelligence on an Australian person outside Australia. This could in turn, raise doubt about the legality of the retention of the intelligence produced; and any subsequent uses to which it may be put, including its evidential admissibility;

[20] Richardson Review, vol. 2, 166 [23.9] citing Joint Select Committee on the Intelligence Services, An Advisory Report on the Intelligence Services Bill 2001, the Intelligence Services (Consequential Provisions) Bill 2001 and certain parts of the Cybercrime Bill 2001 (August 2001), [2.16-2.17].
[21] Paragraph 6(1)(e), *Intelligence Services Act 2001* (Cth).
[22] Paragraph 6(1)(2), *Intelligence Services Act 2001* (Cth).
[23] These important preconditions for giving Ministerial authorisation are mainly directed to proportionality: Section 9, *Intelligence Services Act 2001* (Cth).

- **effective power to confer immunity from legal liability**: if a statutory authorisation is granted in accordance with applicable requirements under Part 2 of the ISA, it will generally have the effect of enlivening an immunity in section 14 of the ISA for the individuals through whom the agency acts, in order to produce intelligence under that authorisation.[24]

31. The Richardson Review, in the context of ministerial authorisation to produce intelligence, highlighted the importance of ensuring that the purpose of an intelligence activity is visible:

> *The Review considers that the purpose for which an agency is undertaking an activity is paramount and should be brought to the minister's attention at the time he or she is asked to authorise that activity.*
>
> *It follows, therefore, that ministerial authorisation to produce intelligence is insufficient where an agency is, in fact, undertaking activities to achieve a direct effect in its own right. The Review does not think it is enough that the categories for seeking ministerial authorisation to produce intelligence contemplate or suggest that action will be taken by the relevant agency. In our view, the inference of a response to intelligence is simply not sufficient to ensure ministerial oversight and accountability for direct effects against an Australian person.*[25]

32. The Law Council reiterates the importance of three key design principles in relation to the authorisation mechanism in Part 2 of the IS Act:

- **Ministerial responsibility and accountability must be given primacy in the design of authorisation mechanisms**: In the absence of a judicial authorisation model for intelligence warrants in Australia (in contrast to all other countries in the Five Eyes alliance), Ministerial-level authorisation of the intrusive intelligence collection powers of ISA agencies, in relation to Australian persons, ought to be the default requirement. This should be conveyed clearly in the legislative text and structure of the ISA. A Ministerial approval model is preferable to a model of internal 'self-authorisation' by agency officials. Having regard to the gravity, intrusiveness, and covert nature of the intelligence collection powers of ISA agencies, Ministerial authorisation (in the absence of judicial authorisation) is essential to ensure visibility, responsibility and accountability. The primacy of Ministerial responsibility for the issuance of authorisations was also a significant guiding principle for the Richardson Review;
- **Any ability for agency heads to give internal authorisation should be regarded as an exceptional measure:** any devolution of responsibility for issuing such authorisations to ISA agency heads is properly regarded as an extraordinary measure, which is an exception to the general model of giving primacy to Ministerial responsibility and accountability for the issuance of authorisations to the agency. This power should therefore be limited to clearly defined circumstances of emergency or significant urgency;
- **In all cases, authorisations must be subject to rigorous issuing thresholds, and administrative requirements to facilitate operational oversight (both Ministerial and independent)**: all forms of authorisation under Part 2 of the ISA (that is, both Ministerial and agency head authorisations) should be subject to rigorous statutory thresholds, and other legally binding safeguards relevant to their execution. Key safeguards include statutory record-keeping, reporting and

[24] LCA Comprehensive Review, 1 February 2022 Submission, 13-15.
[25] Richardson Review, vol. 2, 171 [23.29 - 23.30].

notification requirements, which are important in facilitating oversight and accountability in relation to acts done in reliance on Part 2 authorisations, noting that such acts will generally attract the extensive immunities from legal liability under section 14 of the ISA.[26]

Excluding some NIC agencies from oversight of Commonwealth Ombudsman

33. The Law Council supports amendments to the *Ombudsman Act 1976* (Cth) to exclude the Australian Secret Intelligence Service, the Australian Geospatial-Intelligence Organisation, the Australian Signals Directorate, the Office of National Intelligence, and the Defence Intelligence Organisation from the Commonwealth Ombudsman's jurisdiction.

34. The Law Council notes that this amendment formalises current practice and reflects the reasoning of the Richardson Review which noted:

> *The Ombudsman's jurisdiction extends to all NIC agencies, except ASIO, although the Ombudsman advised the Review that it does not exercise its jurisdiction over AIC agencies by convention. The Ombudsman also told us that it is seeking to formalise this position through amendments to its regulations. We think this is essential. Of the NIC agencies, the Ombudsman has only been active in relation to Home Affairs, the AFP, AUSTRAC and the ACIC. Further, from a practical perspective, the Ombudsman is not adequately equipped to protect sensitive national security information.*[27]

35. The Law Council considers it essential that the resourcing of the Inspector-General of Intelligence and Security (**IGIS**) be continually reviewed to ensure it is sufficient to discharge its statutory responsibilities.

36. As a general comment, the Law Council reiterates its support of the overarching finding of the 2017 Independent Intelligence Review (the **IIR**) that centralised and specialised oversight of the National Intelligence Community, in its entirety, is integral to the very concept of this community as a single, national enterprise, constituted by a 'federation' of agencies who work closely together in collecting, analysing and disseminating intelligence.[28] The IIR considered that concentrating intelligence oversight functions in the IGIS, as the existing specialist body responsible for overseeing six of the 10 agencies, was the most effective and efficient means of achieving that outcome.[29]

Contact

37. Please contact Mr Shounok Chatterjee, Policy Lawyer, on 02 6246 3703 or at shounok.chatterjee@lawcouncil.asn.au if you wish to discuss further.

Yours sincerely

Luke Murphy
President

[26] LCA Comprehensive Review, 1 February 2022 Submission, 14-15 [19].
[27] Richardson Review, vol. 3, 243 [40.30].
[28] Law Council of Australia, Submission to the Parliamentary Joint Committee on Intelligence and Security, Intelligence Oversight and Other Legislation Amendment (Integrity Measures) Bill 2020 (4 March 2021) 12 [31].
[29] M L'Estrange and S Merchant, 2017 Independent Intelligence Review: Unclassified Report, (June 2017), 115-116 [7.19] and [7.22]-[7.23].