Law Council
OF AUSTRALIA

Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021

Parliamentary Joint Committee on Intelligence and Security

1 February 2022

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 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 90,000[1] 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 2022 Executive as at 1 January 2022 are:

- Mr Tass Liveris, President
- Mr Luke Murphy, President-elect
- Mr Greg McIntyre SC, Treasurer
- Ms Juliana Warner, Executive Member
- Ms Elizabeth Carroll, Executive Member
- Ms Elizabeth Shearer, Executive Member

The Acting Chief Executive Officer of the Law Council is Ms Margery Nicoll. The Secretariat serves the Law Council nationally and is based in Canberra.

1 Law Council of Australia, *The Lawyer Project Report*, (pg. 9,10, September 2021).

Acknowledgement

The Law Council gratefully acknowledges the input of the following of its expert advisory bodies to this submission:

- National Security Law Working Group;
- National Criminal Law Committee; and
- National Human Rights Committee.

Executive Summary

1. The Law Council welcomes the opportunity to provide this submission to the review by the Parliamentary Joint Committee on Intelligence and Security (**Committee**) of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2020 (**Bill**).

2. The Bill comprises an assortment of discrete and technically complex amendments to the legislation governing six agencies in the National Intelligence Community (**NIC**).[2] The most significant measures are contained in Schedules 1-5. They propose amendments to certain authorisation and governance requirements in the *Intelligence Services Act 2001* (Cth) (**ISA**) with respect to the intelligence collection and related activities of ASIS, ASD and AGO (collectively, the '**ISA agencies'**).

3. Most proposals in the Bill implement selected recommendations of two major reviews of the NIC and its governing legislation—the *2018-19 Comprehensive Review of the Legal Framework of the National Intelligence Community* (**Richardson Review**),[3] and the *2017 Independent Intelligence Review* (**IIR**).[4] However, the measures in Schedule 5 contradict a recommendation of the Richardson Review that they should not proceed. The Richardson Review disagreed with a prior recommendation of the IIR, which supported them.[5] In late 2020, the Government announced its rejection of the relevant Richardson Review recommendation, giving preference to that of the IIR.[6] Further, the Bill contains a small number of measures, most significantly in Schedule 8, which are additional to the matters addressed in the Richardson Review and IIR recommendations.

Key issues and recommendations addressed in this submission

4. This submission focuses on the following proposed amendments to the ISA:

- **Schedules 1-4**: additional grounds and mechanisms of authorisation for ASIS, ASD and AGO to produce intelligence on an Australian person who is outside Australia. These measures implement recommendation 16 of the IIR, as endorsed by the Richardson Review, in recommendations 45, 46 and 52; and
- **Schedule 5**: an expansion of the cooperative regime in section 13B, under which ASIS may produce intelligence on Australians without a Ministerial authorisation (**MA**), for the purpose of supporting ASIO to perform its functions. This scheme is currently limited to collection activities undertaken by ASIS outside Australia. The proposed amendments would extend it to domestic collection activities by ASIS, which are done in support of ASIO (contrary to recommendation 57 of the Richardson Review, as noted above).

5. In relation to **Schedules 1-4**, the Law Council acknowledges that the Richardson Review and IIR supported the necessity of these measures, following scrutiny of the classified operational case advanced by agencies. However, the Law Council has identified some technical issues in the design and drafting of provisions implementing those recommendations. The Law Council proposes targeted

---

[2] Namely, the: Australian Secret Intelligence Service (**ASIS**); Australian Signals Directorate (**ASD**); Australian Geospatial-Intelligence Organisation (**AGO**); Defence Intelligence Organisation (**DIO**); Office of National Intelligence (**ONI**); and Australian Security Intelligence Organisation (**ASIO**). The measures in the Bill affect the functions of DIO, ONI and ASIO to a more limited extent than those of ASIS, ASD and AGO.

[3] Dennis Richardson AO, *Unclassified Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (December 2019), Vols 1-4. In particular, recs 12, 41, 45, 46, 52, 74 & 189.

[4] Michael L'Estrange AO and Stephen Merchant PSM, *Unclassified Report of the 2017 Independent Intelligence Review* (July 2017) (**IIR Report**). In particular, recommendation 16.

[5] *Richardson Review, Vol 2*, recommendation 57 and 163-164 at [22.64]-[22.65]. Cf *IIR Report*, recommendation 18(b) and 106-107 at [6.54]-[6.61], especially [5.59] and [6.61].

[6] Australian Government, *Response to the Richardson Review*, (December 2020), 19 (rec 57 response).

amendments to address apparent instances of statutory overbreadth, ambiguity and potential unintended consequences (**recommendations 1-8**).

6. In relation to **Schedule 5**, the Law Council considers that the extrinsic materials to the Bill do not provide adequate information to publicly establish the necessity of authorising ASIS to operate domestically to collect security intelligence (that is, as a discrete legal entity to ASIO, with a separate operational chain of command and governance arrangements). It is presently open to ASIO to obtain assistance from ASIS in its domestic intelligence operations via existing cooperative mechanisms in its own governing legislation (namely, by seconding ASIS staff members to work on particular operations, thereby performing functions for and on behalf of ASIO). Significant caution is needed, given the conclusion of the Richardson Review that there was 'insufficient evidence before the Review to demonstrate the operational need for such a supporting role onshore in the same way as it is needed offshore',[7] and the brevity of analysis documented in the prior, unclassified IIR report.[8] As a starting point, further public explanation is needed (**recommendation 9**).

Law Council observations on other, more secondary, matters

7. The Law Council also makes some observations of a more secondary nature on:

- **Schedule 8**: extended periods for the suspension of travel documents (from 14 days to 28 days) to enable ASIO to complete its security assessments; and
- **Schedule 9**: expanded criminal and civil immunities for certain computer-related acts carried out by ASIS and AGO staff members.

8. The Law Council's submissions and **recommendation 10** on **Schedule 8** are directed primarily to scrutinising the supporting case for the proposal to double the period of temporary suspension for an Australian or foreign travel document on security grounds; as opposed to implementing administrative measures to improve efficiency in the furnishing of security assessments by ASIO. The Law Council urges caution in assessing the necessity of a proposal to permanently extend a statutory maximum period, where the supporting justification appears to reflect a 'point in time assessment' of matters of agency administration and resourcing.

9. The Law Council's submissions and **recommendation 11** on **Schedule 9** to the Bill reiterate its previous submissions to the Committee on Schedule 2 to the (then) Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**SOCI Bill**), which expanded the immunity in favour of ASD staff alone.[9] The issues raised in the Law Council's previous submission remain outstanding, and apply with equal force to the proposed extension to ASIS and AGO staff in the present Bill.

Measures that do not raise significant issues for the Law Council

10. The Law Council does not hold significant concerns about the proposals in **Schedules 6-7 and 10-14**, which, if enacted, would variously:

- amend aspects of the privacy framework governing the communication of intelligence containing personal information about Australians (**Schedule 10**);
- improve transparency about ASD's practices in using assumed identities, and simplify oversight and accountability arrangements (**Schedule 11**); and
- rectify ambiguities and minor drafting errors (**Schedules 6-7; 12-14**).

---

[7] *Richardson Review, Vol 2*, 164 at [22.65].

[8] *IIR Report*, 106 at [5.59] which documents one sentence of reasoning underlying the recommendation for this significant amendment: 'Moreover, the geographic limitation in section 13B restricts co-operation'.

[9] Law Council of Australia, *Submission to the PJCIS Review of the SOCI Bill*, (February 2021), 97-106. See also: PJCIS, *Advisory Report on the Review of the SOCI Bill*, (September 2021), [3.58]-[3.62] and rec 10.

List of recommendations

11. The Law Council makes 11 recommendations in relation to the measures in Schedules 1-5 and 8-9 to the Bill, which are consolidated below.

12. The Law Council also makes a number of observations on the measures in the remaining schedules to the Bill, which are not the subject of specific recommendations. However, its comments on Schedules 6, 10 (Part 3) and 12 identify some issues that would benefit from further public explanation, which the Committee may wish to pursue with the proponents of the Bill.

Schedule 1: Emergency agency head authorisations

Recommendation 1—seriousness of the risk to an Australian person under ISA s 9D

- **Proposed subsection 9D(1) or (2) of the ISA should be amended to require the agency head to be satisfied that there is a serious or significant risk to safety of an Australian person, as a precondition to issuing the authorisation (in addition to that risk being imminent).**
- **That is, the amendment should align the criteria for granting an authorisation under proposed section 9D more closely with the existing authorisation condition for emergency agency head authorisations under subparagraph 9B(2)(c)(ii) ('serious risk'), or the cancellation condition in proposed section 9D(12) ('significant risk').**

Recommendation 2—explicit requirement in section 9D of the ISA as to the primary purpose for which intelligence is to be produced

- **Proposed subsection 9D(1) of the ISA should be amended to provide that an agency head may only issue an authorisation if they are satisfied that the primary purpose of producing intelligence on the Australian person whose safety is at risk is to assist that person (that is, by seeking to abate the risk to the person's life or safety).**
- **If the primary objective of producing intelligence on the Australian person is, in fact, to gain insight into one or more specified risks to Australia's security, international relations or economic well-being (and the intelligence would only be used in an incidental or secondary way to assist the person) then there should be clear statutory provision that the authorisation mechanism under section 9D is not available in these circumstances. Rather, the agency should be required to proceed under the authorisation mechanisms in existing sections 9, 9A or 9B of the ISA (as applicable).**

Recommendation 3—maximum period of effect of ISA section 9D authorisations

- **Proposed paragraph 9D(9)(a) of the ISA should be amended to provide that an authorisation issued under section 9D has a maximum period of effect of 48 hours. Proposed subsection 9D(6) should also be amended to require the responsible Minister to specifically consider whether the section 9D authorisation should be replaced with an MA under section 9 or 9A, in addition to considering whether to cancel it under proposed subsection 9D(10).**
- **In this way, the new agency head authorisation mechanism in proposed section 9D would reflect the primacy of Ministerial responsibility and accountability in the same way as the agency head authorisation mechanism in existing section 9B.**
- **Accordingly, all of the agency head authorisation mechanisms in the ISA would ensure that an authorisation given by an agency head could only remain in force until such time as the responsible Minister for the agency could determine whether to authorise the agency's intrusive intelligence collection activities.**

Recommendation 4—requirements for the issuance of ISA section 9D authorisations in relation to Australian children

- **Proposed subsection 9D(1) of the ISA should be amended to provide specific statutory requirements, at least at a high-level, in relation to authorisations to produce intelligence on an Australian child.**
- **The objective of such statutory guidance should be to remove any possibility that section 9D could be capable of authorising an ISA agency to produce intelligence on an Australian child, in circumstances in which the agency would be required to seek an authorisation under section 9, 9A or 9B of the ISA to produce intelligence on an Australian adult.**
- **In particular, there should be:**
  - **an explicit requirement for the agency head to take into account the best interests of the child, consistent with Australia's obligations under the *Convention of the Rights of the Child*, when deciding whether to issue an authorisation under proposed section 9D. (This should not be left solely to the general requirement in proposed paragraph 9D(2)(a) and supporting instruments such as Ministerial directions made under section 8 of the ISA, or operational policies);**
  - **specific statutory guidance on the assessment of whether there is an imminent risk to the child's safety under proposed paragraph 9D(1)(a) by reason of the child's developmental and legal status as a minor; and**
  - **specific statutory guidance on the application of the consent requirements in proposed paragraphs 9D(1)(c) and (d) in circumstances in which a child may be assessed as lacking legal capacity to consent to the production of intelligence, because of their status as a minor (as distinct to practical limitations on the ability of the agency to make contact with the person).**

Recommendation 5—power of delegation in ISA subsection 9D(14)

<u>Preferred option</u>

- **The agency head's power of delegation in proposed subsection 9D(14) of the ISA should be amended to exclude the power to issue an emergency authorisation under proposed subsection 9D(2).**

Alternative option

- **If the Committee is persuaded that ISA agency heads should be able to delegate their power to issue authorisations under proposed subsection 9D(2), the power of delegation in proposed subsection 9D(14) should be amended to further limit the class of prospective delegates.**
- **This class should be defined as staff members of the agency (excluding contractors or consultants) who hold a position which is classified as a prescribed level of seniority, potentially in an analogous manner to the definition of a 'senior position holder' in section 4 of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act).**

Schedule 2: Counter-terrorism class authorisations

Recommendation 6—circumstances in which a person is taken to be 'involved with' a terrorist organisation under proposed ss 9(1AAA) and 9(1AAB) of the ISA

- **Consideration should be given to exhaustively defining the circumstances in which a person is taken to be 'involved with' a terrorist organisation for the purpose of the class authorisation ground in proposed subsection 9(1AAA). In particular, consideration should be given to transforming the illustrative list of circumstances in proposed subsection 9(1AAB) into an exhaustive definition, noting the significant breadth of those activities.**
- **In any event, consideration should be given to amending the deemed grounds of 'involvement' in proposed paragraphs 9(1AAB)(e) and (f) so that they only cover the provision of 'non-financial support' to a terrorist organisation, or 'advocacy' for and on behalf of that organisation which is likely to be material to the organisation's engagement in, or capacity to engage in, terrorism-related activities.**

Schedule 3: Class authorisations for Australian Defence Force (ADF) support

Recommendation 7—Maximum period of effect for Defence Minister's requests to provide assistance to the ADF in overseas military operations

- **Paragraph 9(1)(d) of the ISA should be amended to apply a six-month maximum period of effect to written requests made by the Defence Minister for an ISA agency to provide assistance to the ADF in support of military operations outside Australia.**

Schedule 4: Altered meaning of 'producing intelligence'

Recommendation 8—uncertain meaning of 'covert and intrusive' activities in new subsection 8(1B) of the ISA

- **The Government should provide further explanation of the policy intent, in relation to whether the types of activities discussed at**

paragraphs [137]-[156] of this submission are intended to be characterised as 'covert and intrusive' and therefore subject to the requirement to obtain prior Ministerial authorisation. (That is, geospatial intelligence collection, human intelligence collection including the use of covert human intelligence sources, accessing telecommunications data, and interrogating bulk personal datasets.)

- **Consideration should be given to amending the Bill to provide further statutory guidance about the meaning of the expression 'covert and intrusive' in proposed subsection 8(1B) of the ISA. This could potentially include some of the relevant factors set out in section 26 of the *Regulation of Investigatory Powers Act 2000* (UK).**

Schedule 5: Extension of ASIS-ASIO cooperative regime

Recommendation 9—further information about the necessity and implications of the proposed repeal of paragraph 13B(1)(b) of the ISA

- **Further information should be provided about the necessity of the proposal to enable ASIS to undertake domestic intelligence collection under section 13B of the ISA. It should address the following matters:**
  - **the reasons that it is not considered practicable for ASIO to utilise the operational assistance of individual ASIS staff members as secondees to ASIO ('ASIO affiliates'), and why ASIS should be permitted to act in its own legal capacity (with its own operational command and governance arrangements);**
  - **how risks of overlap, conflict, inconsistency or lack of coordination—which may arise from two agencies operating domestically to collect the same kinds of intelligence—will be managed in practice; and**
  - **why there is no Ministerial involvement in the approval process for ASIS to collect domestic security intelligence in support of ASIO under section 13B of the ISA (as amended); notwithstanding that ASIO requires ministerial approval under section 27B of the ASIO Act to collect foreign intelligence in Australia (even though the collection activities do not require authorisation under a warrant).**

Schedule 8: Timeframe for suspension of travel documents

Recommendation 10—Necessity of proposed doubling of suspension timeframe

- **Further information should be provided about the necessity of the proposal to double the maximum period of interim suspension of Australian or foreign travel documents.**
- **In particular, further information should be provided as to why a permanent doubling of the statutory maximum period of effect is needed in preference to taking administrative action (such as increasing and re-prioritising resources) in order to meet the 14-day time period. This should include explanation of why any spike in current caseload is anticipated to be ongoing or sufficiently long-term as to justify statutory intervention (which will last indefinitely).**
- **While it may be necessary for the Committee to obtain such evidence in camera, by reason of its classified nature, consideration should be given to placing on the public record as much additional information**

as possible about the necessity of the proposed amendments, as distinct to gains in convenience or efficiency.

Schedule 9: Expanded immunities for computer-related acts

Recommendation 11—Implementation of the Committee's recommendation 10 on the SOCI Bill, in relation to ASD, ASIS and AGO

- **The Government should implement recommendation 10 in the Committee's advisory report on the SOCI Bill, in relation to the expansion of the immunity in Division 476 of the *Criminal Code Act 1995* (Cth) (Criminal Code) in favour of ASD staff members, and the proposed expansion in favour of ASIS and AGO staff members.**

Schedule 1: Emergency agency head authorisations

Key proposed amendments

13. Schedule 1 to the Bill proposes to amend Part 2 of the ISA in two key respects:

- **New ground of authorisation:** Schedule 1 would create a new ground upon which ASIS, ASD and AGO can obtain authorisation to produce intelligence on certain Australian persons who are outside Australia. In particular, it would be available in the following circumstances:
  - there is, or is likely to be, an imminent risk to the safety of an Australian person who is physically located outside Australia;
  - it is necessary or desirable to undertake an activity or a series of activities in order to produce intelligence on that person;
  - it is not reasonably practicable to obtain that person's consent to the production of intelligence on them; and
  - having regard to the nature and gravity of the risk to the person's safety, it is reasonable to believe that the person would have consented if they were able to do so.[10]
- **New authorisation mechanism:** Schedule 1 would additionally establish a new mechanism by which ASIS, ASD and AGO can obtain an authorisation in reliance upon the new ground outlined above. The proposed amendments would effectively devolve responsibility from the relevant Minister with portfolio responsibility for the agency—being the Minister for Foreign Affairs (**Foreign Minister**) for ASIS, and the Minister for Defence (**Defence Minister**) for ASD and AGO—to the head of the relevant agency (or a staff member of the agency to whom the agency head has delegated their power).[11]

Legal significance of authorisation mechanisms under Part 2

14. The authorisation mechanisms under Part 2 of the ISA operate as conditions precedent to the performance by ISA agencies of their functions and exercise of their powers to produce intelligence on Australian persons outside Australia. Accordingly, these mechanisms are legally significant in two key respects.

Condition precedent to all intelligence collection on an Australian person

15. First, the authorisation requirements in Part 2 are imposed irrespective of whether the relevant activity or activities sought to be carried out would otherwise constitute an offence or a civil wrong under applicable Australian laws. That is, an ISA agency may be required to obtain a specific statutory authorisation in order to undertake activities to produce intelligence on an Australian person, which a private individual could lawfully carry out. This might include, for example, observing the activities of an Australian person, while that person is in a public place outside Australia.

16. 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 in

[10] Bill, Schedule 1, item 2 (inserting new subsection 9D(1) of the ISA).

[11] Ibid, Schedule 1, item 2 (inserting new subsection 9D(2) of the ISA). See also new subsection 9D(14) (inserted by the same amending item in the Bill) for ISA agency heads' powers of delegation.

legal proceedings—for example, if that intelligence is subsequently shared with law enforcement agencies for the purposes of criminal investigation and prosecution.

Effective power to confer immunity from legal liability

17. Secondly, 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. The immunity in section 14 removes any criminal or civil liability which may otherwise apply to those persons, in respect of acts done in the course of, and as part of, the 'proper performance' by the relevant ISA agency of its functions.[12]

18. In practical terms, where an ISA agency seeks to engage in activities that would otherwise be unlawful for the purpose of producing intelligence on an Australian person outside Australia, the ultimate effect of the applicable statutory authorisation mechanism in Part 2 of the ISA is substantially the same as the 'lawful authority' conferred under warrants issued to law enforcement agencies and ASIO, in respect of intrusive collection activities undertaken as part of their domestic criminal or security intelligence investigations. Consequently, the authorisation provisions under the ISA can fairly be characterised as, in effect, conferring a power on the relevant authorising officer to grant civil and criminal immunities in respect of intrusive intelligence collection activities on Australian persons who are outside Australia. The authorisation requirements in Part 2 of the ISA are not merely a technical condition precedent to the performance of functions by an ISA agency, but rather extinguish existing legal liabilities and corresponding rights of third parties to compensation for loss, damage or injury.

19. This characterisation of the power to grant an authorisation underscores the importance of three legislative design features in relation to all of the authorisation mechanisms in Part 2 of the ISA, including the new agency head authorisation ground proposed in new section 9D. Namely:

- **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;[13]
- **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. As such, this power should be limited to clearly defined circumstances of emergency or significant urgency. (That is, this

[12] Note that the immunity in section 14 of the ISA is also subject to a geographical nexus. Subsection 14(1) covers all acts done outside Australia which are in the proper performance of functions by an ISA agency. Subsection 14(2) also provides a more limited immunity for certain acts done inside Australia, provided that they are preparatory or ancillary to acts done outside Australia.

[13] Richardson Review, *Unclassified Report, Vol 1*, 51 at [3.101].

devolution of the power to confer immunities should be constrained to circumstances in which the time required to obtain Ministerial level authorisation in the normal way would be likely to frustrate, or prejudice significantly, the ability of the agency to collect certain intelligence, which must be of a kind that is highly significant to a specified objective that is in the national interest); and

- **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 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.

Applicable safeguards

20. Having regard to the implications of all Part 2 authorisation mechanisms outlined above, the Law Council is pleased that the proposed authorisation mechanism in new section 9D would be subject to several, significant statutory safeguards. These safeguards are variously contained in existing provisions of the ISA applying to Part 2 authorisations generally, and are proposed to be supplemented by further requirements applying specifically to authorisations under new section 9D.

21. Key safeguards include the following measures:

- the limitations on agencies' functions and activities in existing sections 11 and 12 of the ISA. This includes:
  - explicit prohibitions on the carrying out of policing and law enforcement functions;
  - a requirement that activities may only be carried out in the interests of Australia's national security, foreign relations or economic well-being, and only to the extent they are affected by the capabilities, intentions or activities of persons or organisations outside Australia; and
  - a prohibition on carrying out activities unless they are necessary for the proper performance of the agency's functions, or authorised or required by or under another Act.
- requirements that the agency head responsible for giving the emergency authorisation under proposed section 9D must be satisfied that:
  - the activities sought to be undertaken in reliance on the authorisation will be necessary for the proper performance by the agency of its functions; and
  - there are satisfactory arrangements in place to ensure that the activities will not exceed what is necessary to do so, and the nature and consequences of those acts is reasonable having regard to the purposes for which the activities are carried out;[14]
- notification and reporting requirements, including the following (which replicate the requirements under existing section 9B of the ISA for emergency agency

[14] Bill, Schedule 1, item 2 (inserting proposed paragraph 9D(2)(a) of the ISA, which effectively imports equivalent requirements to those in existing subsections 9A(1) and (1A) for MAs).

head authorisations, if relevant Ministers with power to issue MAs under section 9 or 9A are not readily available or contactable):

- a requirement for the ISA agency head to notify the responsible Minister within a maximum of eight hours that a section 9D authorisation was given, and to provide the relevant documentation within 48 hours (including the instrument of authorisation or a written record of an oral authorisation);[15]

- an obligation on the Minister to decide, as soon as practicable after receiving the documentation, whether to cancel the section 9D authorisation issued by the agency head, and to notify the Inspector-General of Intelligence and Security (**IGIS**) if the Minister exercises the power of cancellation;[16]

- an obligation on the agency head to notify and give copies of relevant documentation to the IGIS;[17]

- an obligation on the IGIS to review and report to the responsible Minister on the agency's compliance with the requirements of section 9D, within 30 days of receiving notification;[18]

- a further obligation on the IGIS to provide the Committee with a copy of the conclusions in the report to the Minister on the agency's compliance with the requirements of section 9D;[19] and

- a requirement for the agency head to provide a report to the Minister on all of the activities carried out in reliance on the section 9D authorisation, within one month of that authorisation ceasing to have effect. (The authorisation may cease to have effect due to its expiry after the six-month maximum period of time, or a shorter expiry date specified in the authorisation. Or it may be revoked sooner by the agency head, or cancelled by the Minister).[20]

Review findings on limitations in the existing emergency authorisation mechanisms under the ISA

Existing mechanisms

22. The ISA already contains emergency authorisation provisions in sections 9A and 9B, which truncate the usual procedural requirements for obtaining an MA under section 9 to enable the production of intelligence on an Australian person who is outside Australia. The intent of these existing provisions is to accommodate various circumstances of urgency, in which the time required to obtain an MA via the usual process in section 9 would frustrate or compromise significantly an intelligence collection opportunity.[21]

23. The emergency authorisation provisions are available if the responsible Minister for the relevant ISA agency is not readily available or contactable, in which case the senior Minister with portfolio responsibility for another ISA agency, or the

[15] Ibid (inserting proposed subsection 9D(4) and paragraph 9D(5)(c) of the ISA).
[16] Ibid (inserting proposed subsection 9D(6) of the ISA).
[17] Ibid (inserting proposed paragraph 9D(5)(d) of the ISA).
[18] Ibid (inserting proposed paragraphs 9D(8)(a) and (b) of the ISA).
[19] Ibid (inserting proposed paragraph 9D(8)(c) of the ISA).
[20] Ibid, Schedule 1, item 3 (amending subsections 10A(1) and (4) of the ISA).
[21] See, for example: Explanatory Memorandum, Counter-Terrorism Legislation Amendment Bill (No. 1) 2014, [209] (explanation of section 9B of the ISA).

Attorney-General, Home Affairs Minister or Prime Minister, may orally grant the authorisation, which is effective for a limited period of up to 48 hours.[22]

24. The existing emergency authorisation mechanisms in the ISA also contain contingency arrangements if none of the above Ministers are readily available or contactable. In this event, the head of the relevant ISA agency may grant a limited authorisation, which is effective for a maximum of 48 hours, if certain criteria are met. In recognition of their exceptional nature, these emergency agency head authorisations are subject to further statutory notification and reporting requirements to the responsible Minister (who must also decide whether to cancel it or replace it with an MA under section 9 or 9A), the IGIS and the Committee.[23]

25. The emergency agency head authorisation regime, in existing section 9B of the ISA, was enacted in 2014 in response to an operational need identified by ISA agencies for an expedited mechanism in circumstances of emergency which included, but were not limited to, imminent threats to the life and safety of Australian persons outside Australia. This mechanism was also intended to be capable of covering other circumstances which were determined to constitute an emergency—for example, instances in which there was an extremely limited window for the collection of important intelligence, which would have been lost or compromised due to the time taken to obtain an MA via the usual statutory process in section 9.[24]

Review findings

26. Both the Richardson Review and the IIR concluded, on the basis of operational evidence provided by agencies to those reviews, that the existing emergency provisions in the ISA, including the agency head authorisation mechanism in section 9B, have not operated optimally in circumstances of extreme emergency, namely where:

- the life or safety of an Australian person was at imminent risk;
- the immediate or near-immediate production of intelligence on that person was assessed as being reasonably likely to have assisted in reducing that risk; and
- it was reasonable to believe that the Australian person whose life or safety was at risk would likely have consented to the production of intelligence on them, if it had been reasonably practicable to seek their consent.

27. The reviews specifically had in their contemplation a scenario in which an Australian person was kidnapped, taken hostage or otherwise arbitrarily detained overseas—for example, by a terrorist organisation in a foreign conflict zone. As the Richardson Review commented at [21.49]-[21.51] of its unclassified report (citations omitted):

> *21.49 The application of the IS Act emergency authorisation provisions to hostage situations was considered by the 2017 Independent Intelligence Review (2017 IIR). The 2017 IIR stated that 'the application of the [ministerial authorisation] regime in relation to operations designed*

[22] ISA, section 9A.

[23] Ibid, section 9B. (Note also the mechanism in section 9C, which applies where the agreement of the Attorney-General is required to the issuance of an under paragraph 9(1A)(b) because the Australian person or persons being targeted are suspected of being involved in activities which are threats to Australia's national security. Section 9C provides a mechanism for the Director-General of Security to give the requisite agreement to the issuance of the MA, if the Attorney-General is not readily available or contactable.)

[24] *Counter-Terrorism Legislation Amendment Act (No. 1) 2014* (Cth), Schedule 2, item 18. See also: PJCIS, *Advisory Report on the Counter-Terrorism Legislation Amendment Bill (No. 1) 2014*, (November 2014), 32 at [3.10], 49-50 at [3.74]-[3.76], and 53 at [3.83].

> *to help ensure the safety of individual Australians' is a 'problematic area of the ISA':*
>
> > *These are operations where it is in the interests of the Australian person that the capabilities of the ISA agencies be used to produce intelligence about their activities or whereabouts. The clearest example is where an Australian is kidnapped or taken hostage, and could also include situations where an Australian person is in arbitrary detention overseas. At present ASIS and ASD are required to seek an MA before undertaking an activity to produce intelligence which may, for example, help identify where that person may be, who may have kidnapped them and that intermediaries may be involved. In these types of circumstances, time can be of the essence and the MA process, including the emergency authorisation provisions, can be an unnecessary delay.*
>
> ***
>
> *21.50 Hostage situations are readily distinguishable from the vast majority of emergency authorisations … in that they are situations where it is reasonable to believe a person would consent to the … agency producing intelligence on them.*[25]

28. Importantly, it is evident from such remarks that the policy intent underlying the amendments is to effectively create a 'backstop', which is directed solely to enabling the expeditious production of intelligence in very narrowly defined circumstances, which are highly time-critical and raise a high level of risk to life or limb. The Law Council welcomes that there is no apparent policy intention for these proposed amendments to effectively replace the primary position under the ISA in relation to Ministerial responsibility and accountability for granting authorisations, which must be obtained in advance of an agency doing any act for the purpose of, or purposes including, the production of intelligence on an Australian person who is outside Australia.[26] This is consistent with the emphasis that the Committee, as it was constituted in 2014, placed upon the ISA giving clear effect to the principle of Ministerial responsibility and accountability for approving the intrusive intelligence collection activities of ISA agencies.[27]

Law Council views

Necessity

29. Given the findings of both reviews, based on evidence of agencies' operational experience, that the existing emergency authorisation provisions have not operated optimally in circumstances of extreme emergency involving hostage-type situations, the Law Council has no 'in-principle' objection to the conferral of a new authorisation ground and mechanism.

30. However, from a rule of law perspective, the major legislative scrutiny issue is whether the proposed provisions giving effect to the recommendations of the IIR and Richardson Review are proportionate to the legitimate operational objectives to which they are directed. A key issue is the extent to which the proposed

[25] Richardson Review, *Unclassified Report, Vol 2*, 147-148 at [21.49]-[21.50] and recommendation 52.

[26] Note, for completeness, that ASIS also requires an MA to do any act which is likely to have a 'direct effect' on an Australian person who is outside Australia, for the purpose of performing its function under paragraph 6(1)(e) of the ISA to 'undertake such other activities as the [Foreign Minister] directs relating to the capabilities, intentions or activities of people or organisations outside Australia': ISA, subparagraph 8(1)(a)(ii). ASIS is unique in having the 'direct effects' MA ground, which reflects that ASD and AGO do not have a corresponding function to that of ASIS under subsection 6(1)(e) of the ISA.

[27] PJCIS, *Advisory Report on the Counter-Terrorism Legislation Amendment Bill (No. 1) 2014*, (November 2014), 49-50 at [3.74]-[3.76].

amendments give effect to the intention to create a narrowly defined exception to the general requirement for agencies to obtain an MA, in the specific circumstances contemplated by the reviews, and are not capable of a broader application, especially if it is unintended. This matter is discussed below.

Proportionality

31. The Law Council has identified five main issues in the design and drafting of proposed section 9D of the ISA, which tend against a conclusion that the proposed authorisation mechanism meets the essential requirements of proportionality. These matters are outlined below, including recommendations for targeted amendments to provisions of the Bill to remedy them.

Issuing grounds—significance of apprehended risk to an Australian person

32. Proposed paragraph 9D(1)(a) provides that an authorisation may be granted if the agency head is satisfied that there is, or is likely to be, an imminent risk to the safety of an Australian person who is outside Australia.

33. There is no requirement that the agency head must also assess the nature and degree of the imminent risk to the person's safety, and be satisfied that it is sufficiently serious as to warrant the exercise of powers in the absence of an MA (in addition to being satisfied of the imminence of that risk). For example, there is no requirement to be satisfied that there is a risk of death or serious harm to the person. Rather, proposed subsection 9D(12) obliges the agency head to cancel an authorisation which has already been issued, if satisfied that there is not, and is not likely to be, a significant risk to the safety of an Australian person.

34. While the authorisation criterion in proposed paragraph 9D(1)(d) requires the agency head to have regard to the nature and gravity of the risk to the safety of the Australian person concerned, this assessment is required only in the context of considering whether the Australian person would likely have consented to the production of intelligence, had it been reasonably practicable to seek their consent. There is no explicit, stand-alone requirement for an objective assessment of the significance of the risk, for the purpose of determining whether it is appropriate to proceed under section 9D, to the exclusion of obtaining an ordinary MA under section 9, or one of the other emergency authorisations in section 9A (Ministerial) or section 9B (agency head) which require an assessment that the relevant Minister or Ministers are not readily available or contactable.

35. This proposed approach to the conditions for the granting of a section 9D authorisation stands in contrast to the statutory condition in existing subparagraph 9B(2)(c)(ii) for the granting of an emergency agency head authorisation where no relevant Ministers are readily available or contactable. The latter provision requires the agency head to be satisfied that, if an emergency authorisation is not granted, there will be or is likely to be 'a serious risk to the person's safety'.

36. The Explanatory Memorandum to the Bill does not address the reasons that a different approach has been adopted in relation to the conditions for the new authorisation mechanism in proposed paragraph 9D(1)(a) or subsection 9D(2). The Law Council considers that an express requirement to assess, and be satisfied of, the significance of risk to the safety of an Australian person should be included in the conditions for the granting of a section 9D authorisation in proposed subsection 9D(1), in addition to the conditions in proposed subsection 9D(12) which trigger the obligation to cancel such an authorisation.

37. The Law Council notes that the Explanatory Memorandum to the Bill also appears to contemplate that an authorisation under proposed section 9D would only be granted if it is assessed that there is a significant risk to the safety of an Australian person. In explaining the reasons that the authorisation criterion in proposed

paragraph 9D(1)(a) applies to an 'imminent risk', but the cancellation obligation in proposed subsection 9D(12) applies to a risk that is 'not significant', the Explanatory Memorandum states that 'there may be situations where it is important that the intelligence continue to be gathered while the risk remains significant, even if, in the circumstances, that risk may no longer be imminent' (emphasis added).[28]

38. In other words, for a risk to be assessed as remaining significant in the context of deciding whether there is an obligation to cancel a section 9D authorisation (as described in the passage of the Explanatory Memorandum quoted above), there must necessarily have been an assessment that the risk was significant when the authorisation was first granted. However, there is no explicit statutory authorisation criterion directed to ascertaining the significance of the risk matter in proposed subsection 9D(1) or (2).

39. The Law Council's recommendation for the insertion of an explicit authorisation criterion in proposed subsection 9D(1) or (2) that the risk must be objectively assessed as 'significant' would give clear effect to that apparent policy intention.

40. This recommendation would also remove the legal risk in the interpretation of section 9D that no such requirement applies. This risk could arise as a matter of statutory interpretation, because of the presence of an express requirement to assess and be satisfied of the seriousness of the risk in the separate ground of agency head authorisation in existing subparagraph 9B(2)(c)(ii); and the absence of an equivalent requirement in proposed subsection 9D(1) or (2). This could be taken to evince an intention that the conditions for the issuance of a section 9D authorisation do not require an objective assessment of the degree of risk to the safety of the relevant Australian person, as is currently required for section 9B authorisations.

Recommendation 1—seriousness of the risk to an Australian person under s 9D

- **Proposed subsection 9D(1) or (2) should be amended to require the agency head to be satisfied that there is a serious or significant risk to safety of an Australian person, as a precondition to issuing the authorisation (in addition to the risk being imminent).**
- **That is, the amendment should align the criteria for granting an authorisation under proposed section 9D more closely with the existing authorisation condition for emergency agency head authorisations under subparagraph 9B(2)(c)(ii) ('serious risk'), or the cancellation condition in proposed section 9D(12) ('significant risk').**

Authorised activities

41. As noted above, the IIR and Richardson Review recommended the enactment of a new agency head authorisation mechanism to enable the production of intelligence on an Australian person, in order to help Australian agencies attempting to bring them to safety, where it is reasonable to believe that the person would have consented to this action, if it had been reasonably practicable to seek their consent.

42. The Law Council considers that it would be beneficial for proposed subsection 9D(1) to give clearer expression to this policy intent. In particular, proposed paragraph 9D(1)(d) prescribes a condition that it is reasonable to believe the person would have consented to the production of intelligence on them. However, there is no explicit requirement that a section 9D authorisation can only be granted

[28] Explanatory Memorandum, 57 at [40].

if the primary purpose of producing that intelligence is to assist the Australian person—that is, by seeking to remove or reduce the identified risk to their safety.[29]

43. This may create a possibility in which a section 9D authorisation could be utilised—in preference to seeking an ordinary MA under section 9, or another emergency authorisation under section 9A or 9B—to enable the production of intelligence on an Australian person for reasons that are not directed primarily to assisting them, but rather may only do so incidentally or as a secondary objective, as part of an intelligence operation which is focused on other priorities.

44. For example, if an Australian person is engaged in activities which concern Australia's security, international relations or economic well-being, and is also taken hostage or otherwise arbitrarily detained overseas, an agency may seek to produce intelligence on them for multiple purposes which could include, but also extend far beyond, assisting that person to escape a risk to their life or safety. Indeed, it is possible that the primary purpose or motivation for seeking to produce the relevant intelligence may be to obtain further insight into a specific risk to Australia's security, or a matter affecting its foreign relations or national economic well-being. However, it might also be reasonably open to the agency head to be satisfied, under proposed paragraph 9D(1)(d), that the Australian person would have consented to the production of intelligence on them, because that intelligence may also have some degree of utility in helping to abate a risk to their safety, even if it was not the priority or primary motivation for the agency seeking to produce the intelligence on the person.

45. The Law Council has no 'in principle' objection to there being a power to produce intelligence on such an Australian person for multiple purposes in such circumstances. However, there is an open question as to whether it should be legally possible for proposed section 9D to provide the authorisation mechanism in this situation, given that it devolves authority from the Minister to the agency head.

46. Alternatively, where the primary objective in producing intelligence on an Australian person is not to assist them by seeking to abate a risk to their safety, consideration could be given to inserting provisions in Part 2 the ISA, which would make clear that the agency must proceed under a different authorisation mechanism with more stringent issuing requirements, including Ministerial-level authorisation wherever one of the relevant Ministers is readily available and contactable.

47. The Law Council's preference is that it should not be possible to obtain an internal authorisation under section 9D where the intended production of intelligence on an Australian person is not for the primary purpose of attempting to reduce a risk to that person's life or safety. This would appear to exceed the intent of the underlying review recommendations to confer a new authorisation mechanism, which relieves the agency of the requirement to obtain Ministerial-level approval, or attempting to obtain such approval, before being able to proceed to internal agency approval.

48. Accordingly, the Law Council recommends that the authorisation criteria in proposed subsection 9D(1) should be amended to include an explicit prohibition on section 9D being utilised in this way, so that the matter is placed beyond doubt or argument in future.

49. The Law Council acknowledges that it may be open to the responsible Ministers for the ISA agencies to address this matter via the directions they are obliged to give to agency heads under subsection 8(1) concerning requirements to obtain authorisations under Part 2. For example, the Minister could issue a direction to an

[29] It is acknowledged that proposed paragraph 9D(1)(b) requires the agency head to be satisfied that doing an activity or series of activities is 'necessary or desirable' for the purpose of producing intelligence on the Australian person. However, the requirement in relation to assessing necessity and proportionality is not directed to an examination of the purpose to which the intelligence will be put.

ISA agency head, stating that the agency is required to obtain an MA under section 9 or 9A, or an emergency authorisation under section 9B, to produce intelligence on an Australian person whose safety is at imminent risk, but the primary purpose of the intelligence production is not to attempt to abate that risk. (That is, the Minister could direct the agency not to rely upon section 9D in such instances.)

50. However, the Law Council considers that the interests of transparency and certainty would be served more effectively via the amendment of the statutory authorisation criteria in proposed subsection 9D(1). Reliance on the exercise of discretion by individual Ministers holding office from time-to-time to issue directions under subsection 8(1) would not provide the public with significant assurance. Those directions are not legislative instruments,[30] and are not otherwise made public because of their classified nature. They are also subject to unilateral revocation or variation at the Minister's discretion.

Recommendation 2—explicit requirement in section 9D as to the primary purpose for which intelligence is to be produced on the Australian person

- **Proposed subsection 9D(1) of the ISA should be amended to provide that an agency head may only issue an authorisation if they are satisfied that the primary purpose of producing intelligence on the Australian person whose safety is at risk is to assist that person (that is, by seeking to abate the risk to the person's life or safety).**
- **If the primary objective of producing intelligence on the Australian person is, in fact, to gain insight into one or more specified risks to Australia's security, international relations or economic well-being (and the intelligence would only be used in an incidental or secondary way to assist the person) then there should be a clear statutory provision stating that the authorisation mechanism under section 9D is not available in these circumstances. Rather, the agency should be required to proceed under the authorisation mechanisms in existing sections 9, 9A or 9B of the ISA (as applicable).**

Period of effect

51. Proposed subsection 9D(9) provides that a section 9D authorisation may remain in force for up to six months, which is the same maximum duration for an MA issued under section 9.[31] This is provided that the authorisation is not cancelled by the Minister or agency head under proposed subsection 9D(10) or 9D(12).

Inconsistency with the principle of Ministerial responsibility and accountability

52. The Law Council has no 'in-principle' objection to an ISA agency being authorised to produce intelligence on an Australian person whose safety is at risk for up to six months. In the abstract, it appears plausible that hostage or kidnapping events, or other forms of arbitrary detention, could continue for prolonged periods of time.

53. However, there is an outstanding question as to whether a single authorisation, issued by the agency head, should cover the entire period of up to six months, subject only to what is essentially a discretionary Ministerial power of 'veto' (being the exercise of the Minister's cancellation power in proposed subsection 9D(10).

54. The Law Council encourages the Committee to consider whether this approach to the maximum period of effect for section 9D authorisations is compatible with the policy intent of the ISA to place primacy on Ministerial responsibility and accountability for authorising the intrusive intelligence collection activities of ISA

[30] ISA, subsection 8(5).

[31] Ibid, subsection 9(4).

agencies. (This includes authorisation of intelligence collection activities which enliven the application of the immunity from legal liability in section 14 of the ISA, because they would otherwise contravene applicable Australian laws.)
An alternative approach, modelled on that in existing section 9B is available. It is preferable for new section 9D to be consistent with existing section 9B.

Divergence from the approach to section 9B emergency authorisations

55. The maximum period of effect in proposed subsection 9D(9) is considerably longer than the 48-hour maximum period of effect for existing emergency agency head authorisations under existing paragraph 9B(4)(c) of the ISA.[32]

56. The Law Council notes the reasonable possibility that an intelligence collection operation carried out in reliance on an emergency authorisation given under existing section 9B of the ISA may need to continue longer than the 48-hour maximum duration of that authorisation. However, in those circumstances, the responsible Minister for the ISA agency would need to issue an MA under section 9 or 9A, if satisfied the criteria are met, which would replace the section 9B authorisation given by the agency head. Existing paragraph 9B(7)(b) of the ISA expressly requires the Minister to consider whether to issue an MA under section 9 or 9A of the ISA, as soon as practicable after being given a copy of the emergency authorisation granted by the ISA agency head under section 9B.

57. In other words, under the section 9B authorisation mechanism, an ISA agency head's authorisation only remains in force for a temporary period to enable urgent intelligence collection activities to be taken, until such time as the Minister considers whether to issue an MA. This gives clear expression to the principle of giving primacy to Ministerial responsibility and accountability for authorising the intrusive activities of ISA agencies and enlivening statutory immunities.

58. Proposed subsection 9D(6) of the ISA, which sets out the role of the responsible Minister in relation to section 9D authorisations, does not contain an equivalent provision to that in existing paragraph 9B(7)(b) of the ISA. Rather, proposed subsection 9D(6) only obliges the Minister to consider whether to cancel the agency head's authorisation, pursuant to the Minister's cancellation power in proposed subsection 9D(10) of the ISA. It does not also oblige the Minister to consider whether to replace the section 9D authorisation with an MA issued under section 9 or 9A.

59. The extrinsic materials to the Bill do not appear to explain why the proposed section 9D agency head authorisation mechanism departs from this aspect of the existing agency head authorisation mechanism in subsection 9B(7).

60. The Law Council notes that the authorisation criterion in proposed paragraph 9D(1)(a) is directed specifically to circumstances in which the risk to an Australian person's safety is assessed as being 'imminent'. It would be preferable if an authorisation issued by an agency head under proposed section 9D was only capable of remaining in force in the following circumstances:

- only as long as the original issuing criteria in proposed subsections 9D(1) and (2) continue to be satisfied—and, in particular, the requirement in proposed paragraph 9A(1)(a) that the risk to the Australian person's safety is assessed as being imminent; and
- in any case, for a defined and short maximum period of time, which is commensurate with the extraordinary step of devolving such a significant

[32] It is also considerably longer than the 48-hour maximum period of effect for an emergency oral MA, issued under section 9A: ISA, paragraph 9A(4)(b).

authorisation power from the responsible Minister for an ISA agency to an official of that agency.

61. If the ISA agency needs to produce intelligence on the Australian person beyond this limited period of effect, because it considers that the risk to the Australian person's safety remains significant, then the agency should be required seek a fresh MA from a relevant Minister, pursuant to section 9 or 9A of the ISA. The Law Council therefore does not support the specific approach proposed in the Bill, whereby:

- the agency head can grant an authorisation under section 9D if satisfied that there is an imminent risk to the safety of an Australian person: see proposed paragraph 9A(1)(a); and
- if granted, a section 9D authorisation will remain in force for up to six months (an equal maximum duration to an MA issued under section 9) subject to:
  - discretionary cancellation by the Minister, without an express obligation to consider whether to replace the authorisation with an MA, as soon as practicable after being given a copy of the agency head's section 9D authorisation: see proposed subsections 9D(6) and (10); and
  - mandatory cancellation by the agency head, on the basis that the risk is no longer significant (that is, a section 9D authorisation could remain in force even if the original issuing criterion requiring the existence of an imminent risk is no longer met): see proposed subsection 9D(12).

Divergence from emergency authorisations for law enforcement agencies

62. Further, the approach taken to the design of existing section 9B of the ISA (under which agency head authorisations only last for up to 48 hours, and must effectively be replaced with an MA in order for the agency to produce intelligence beyond that period) is also more closely aligned with the requirements for internally issued emergency authorisations issued under legislation conferring intrusive powers on law enforcement agencies.

63. For example, Part 3 of the *Surveillance Devices Act 2004* (Cth) makes provision for the issuance of officer-level authorisations to use surveillance devices where it is not possible to obtain a warrant in advance because of circumstances of emergency. However, such internal authorisations are subject to requirements for the relevant law enforcement officers to subsequently seek external approval from an issuing authority within 48 hours of the issuance of the emergency authorisation.[33] That external approval must be sought retrospectively, in respect of surveillance activities already carried out pursuant to the emergency authorisation. Further, if the issuing authority is satisfied that there is a continued need to use the surveillance device beyond the period covered by the emergency authorisation, they may issue a surveillance device warrant on a prospective basis.[34] This approach similarly places primacy on the external approval of intrusive investigative powers.

64. The Law Council recommends that the new authorisation mechanism in proposed section 9D of the ISA should be compatible with established approaches to the design of emergency authorisations for both intelligence and law enforcement agencies to exercise intrusive powers in relation to Australian persons.

Recommendation 3—maximum period of effect of section 9D authorisations

[33] *Surveillance Devices Act 2004* (Cth), section 33.

[34] Ibid, subsection 35(1)-(3) (retrospective approval) and subsection 35(4) (prospective warrant).

- **Proposed paragraph 9D(9)(a) of the ISA should be amended to provide that an authorisation issued under section 9D has a maximum period of effect of 48 hours. Proposed subsection 9D(6) should also be amended to require the responsible Minister to specifically consider whether the section 9D authorisation should be replaced with an MA under section 9 or 9A, in addition to considering whether to cancel it under proposed subsection 9D(10).**
- **In this way, the new agency head authorisation mechanism in proposed section 9D would reflect the primacy of Ministerial responsibility and accountability in the same way as the agency head authorisation mechanism in existing section 9B.**
- **Accordingly, all of the agency head authorisation mechanisms in the ISA would ensure that an authorisation given by an agency head could only remain in force until such time as the responsible Minister for the agency could determine whether to personally authorise the agency's intrusive intelligence collection activities in relation to Australians.**

Safeguards for children

65. The Law Council notes that the authorisation criteria in proposed subsection 9D(1) may apply differently in relation to the production of intelligence on Australian children, as compared to adults. As explained below, in the absence of explicit statutory authorisation requirements for the production of intelligence on Australian children, it appears possible that the section 9D authorisation mechanism could lawfully enable the production of intelligence on an Australian child, without Ministerial approval, in broader circumstances than may be possible in relation to an Australian adult.

66. As also explained below, the Law Council supports amendments to section 9D to provide further statutory guidance about its application to children. The Law Council acknowledges that it would be open to the responsible Minister for an ISA agency to issue directions to the agency head under subsection 8(1) or 8(2) which deal with the issuance of section 9D authorisations to produce intelligence on Australian children. However, the intrusiveness of the relevant intelligence collection powers, and the enlivenment of broad immunities from legal liability, require a stronger and more transparent safeguard than the exercise of executive discretion to make classified directions, which can be unilaterally revoked or varied.

Application of the consent requirements in proposed paragraphs 9D(1)(c)-(d) to children

67. Proposed paragraph 9D(1)(c) provides that an ISA agency head may only issue an authorisation under section 9D if satisfied that it was not reasonably practicable to obtain the consent of the relevant Australian person whose safety is at risk to the production of intelligence on them. Proposed paragraph 9D(1)(d) further requires the existence of a reasonable belief that the Australian person would have consented to the production of intelligence on them, if they were able to do so.

68. This raises a question about the potential use of section 9D authorisations to produce intelligence on Australian children who are outside Australia. A child may be unable to give consent for reasons of legal incapacity, which arise from their developmental status, rather than the more practical reasons of the kind outlined in the Explanatory Memorandum, which are provided as examples of circumstances in which it is not reasonably practicable to seek consent for the purpose of proposed paragraph 9D(1)(c). Those reasons focus on the inability of the agency to contact the person, including because there are no practicable means to make

contact; or because any contact with the person could compromise their safety or that of agency staff, or the covert nature of an intelligence operation.[35]

69. It is unclear whether proposed paragraph 9D(1)(c) would enable an ISA agency head to conclude that it was not reasonably practicable to seek a child's consent, because the child's developmental and legal status as a minor would preclude them from giving valid and informed consent (even if it were practically possible to make contact with the child, without compromising safety or security of any person, or the operational security of the agency). It is further unclear whether proposed paragraph 9D(1)(d) could enable an agency head to effectively assume that the child had legal capacity to give consent as though they were an adult, and then proceed to make an assessment as to whether the child, if their level of cognitive development and maturity was sufficient, would have been likely to have given their consent to the production of intelligence, in the circumstances known to the agency.

70. The Law Council submits that more detailed statutory guidance is required in relation to the application of the new authorisation mechanism in section 9D in relation to Australian children. This is the first time that an authorisation mechanism in the ISA for the production of intelligence on an Australian person mandates consideration of whether it was reasonably practicable to seek the consent of the target to the production of intelligence on them; and whether the target would have consented to the production of such intelligence had they been able to do so.

71. The Richardson Review appeared to place determinative weight on this consent-related condition as the basis for its recommendation that the new ground of agency head authorisation should proceed.[36] It is therefore important that there is clarity and certainty, on the face of the provisions themselves, about the scope and application of the consent condition. It is particularly important that there is clarity in relation to Australian children, to ensure that the new authorisation mechanism is only capable of being exercised in a manner that is compatible with Australia's international obligations under the *Convention on the Rights of the Child*. These matters should not be left exclusively to classified Ministerial directions given under section 8 of the ISA, or classified operational policies set by the agency head. Rather, at least the high-level requirements in relation to children should be reflected expressly in the statutory scope of the power to issue an authorisation under proposed section 9D.

72. The Law Council suggests that proposed subsection 9D(1) should include specific conditions for the issuance of an authorisation to produce intelligence on an Australian person who is a child. The agency head should be required to specifically consider the best interests of the child, based on all information available to them at the material time, including the nature and gravity of the risk to the child's safety.

The assessment of safety risk in proposed paragraph 9D(1)(a)

73. Further, proposed paragraph 9D(1)(a) provides that an agency head may only issue an authorisation if satisfied that there is an imminent risk to the safety of an Australian person. As noted above, the Richardson Review and IIR contemplated circumstances in which an Australian person is taken hostage, kidnapped or otherwise arbitrarily detained (for example, as part of a mass casualty attack by a terrorist group or another hostile actor).

---

[35] Explanatory Memorandum, 54 at [22].

[36] Richardson Review, *Unclassified Report, Vol 2*, 148 at [21.50]: 'Hostage situations are readily distinguishable from the vast majority of emergency authorisations … in that they are situations where it is reasonable to believe a person would consent to the … agency producing intelligence on them'.

74. However, the safety of an Australian child might be placed at risk in a much broader range of circumstances than an Australian adult, because of the child's special vulnerabilities arising from their developmental status and legal incapacity as a minor. (That is, these attributes might make the child more vulnerable to harm than an adult, particularly with respect to mental harm.)

75. For example, an Australian child who is involuntarily taken to a foreign conflict zone by their parents, because their parents wished to fight with or support a terrorist organisation involved in the conflict, may be exposed to extreme levels of violence and radical ideology, and inadequate health care and other necessities of life. It is arguable that, for these reasons, the child's mental and physical health are at significant risk in the foreign conflict zone. This may provide a basis for an ISA agency to conclude that there is an imminent risk to the child's safety for the purpose of proposed section 9D of the ISA.

76. While the Law Council has no 'in-principle' objection to ISA agencies being empowered to produce intelligence in these circumstances, it questions whether the agency head authorisation mechanism in proposed section 9D should be capable of application in such circumstances in respect of Australian children. This would make it legally possible for an ISA agency to internally authorise the production of intelligence on an Australian child, where it would presently require an MA to do so; and if the Bill were passed in its current form, the agency would likely still require an MA to produce the same intelligence if the Australian child was an adult. Further, if section 9D were capable of application in this manner in relation to Australian children, it would enable an ISA agency head to issue an authorisation to produce intelligence on that child even if the responsible Minister for the agency was readily available and contactable, and could have promptly considered an MA request and issued an MA (including via provisions permitting oral requests and issuance).

77. The Law Council envisages that such an outcome is not the policy intent of proposed section 9D, noting that neither the Richardson Review nor the IIR made recommendations to this effect. This tends in further support of the Law Council's recommendation that proposed section 9D should include explicit guidance on the application of the authorisation criteria to children, rather than leaving this matter exclusively to administrative action (such as the issuance of Ministerial directions to the agency, or internal policies set by the agency head).

78. Similarly, the Law Council submits that this matter should not be left to the exercise of discretion in making decisions about the application of general safeguards in the ISA, such as that in existing subsection 9(1), to specific authorisation requests.[37]

Recommendation 4—requirements for the issuance of section 9D authorisations in relation to Australian children

- **Proposed subsection 9D(1) of the ISA should be amended to provide specific statutory requirements, at least at a high-level, in relation to authorisations to produce intelligence on an Australian child.**
- **The objective of such statutory guidance should be to remove any possibility that section 9D could be capable of authorising an ISA agency to produce intelligence on an Australian child, in circumstances in which the agency would be required to seek an**

[37] Existing subsection 9(1) provides that the responsible Minister may only issue an MA to the relevant ISA agency if satisfied that any activities carried out under the MA will be necessary for the proper performance of the agency's functions; and that there are satisfactory arrangements in place to ensure the necessity, proportionality and reasonableness of those activities, having regard to the purposes for which they are carried out. Proposed paragraph 9D(2)(a) provides that the agency head can only issue an authorisation if the facts of the case would justify the responsible Minister giving an MA under section 9, because the conditions in subsection 9(1) and 9(1A) are met.

authorisation under section 9, 9A or 9B of the ISA to produce intelligence on an Australian adult.

- **In particular, there should be:**
  - **an explicit requirement for the agency head to take into account the best interests of the child, consistent with Australia's obligations under the *Convention of the Rights of the Child*, when deciding whether to issue an authorisation under proposed section 9D. (This should not be left solely to the general requirement in proposed paragraph 9D(2)(a) and supporting instruments such as Ministerial directions made under section 8 of the ISA, or operational policies);**
  - **specific statutory guidance on the assessment of whether there is an imminent risk to the child's safety under proposed paragraph 9D(1)(a) by reason of the child's developmental and legal status as a minor; and**
  - **specific statutory guidance on the application of the consent requirements in proposed paragraphs 9D(1)(c) and (d) in circumstances in which a child may be assessed as lacking legal capacity to consent to the production of intelligence, because of their status as a minor (as distinct to practical limitations on the ability of the agency to make contact with the person).**

Powers of delegation

79. Proposed subsection 9D(14) provides that the head of ASIS, ASD or AGO may delegate any or all of their powers, functions and duties under proposed section 9D to any staff member of their agency, excluding consultants or contractors. This would include the power to issue an emergency authorisation under proposed subsection 9D(2) and not merely the performance of other functions or duties relevant to section 9D authorisations (such as complying with record-keeping requirements, and other obligations to notify and provide documentation the responsible Minister and IGIS).

80. The breadth of this power of delegation appears inconsistent with the expression of policy intent in the Explanatory Memorandum to the Bill. The Explanatory Memorandum states that the power of delegation extends only to 'certain select staff members, as opposed to that authority being vested in all staff members of the agency'.[38] In fact, proposed subsection 9D(14) only excludes limited classes of staff members from the pool of prospective delegates, by reference to the legal mechanisms by which those staff members were engaged by the agency (that is, as consultants or contractors). It would be legally possible to delegate the power to issue an emergency authorisation under subsection 9D(2) to any employee of the agency (including classes of agency employees)[39] at the complete discretion of the agency head (subject perhaps only to the administrative law doctrine of unreasonableness, which applies a very high threshold).[40]

81. The Law Council considers that the power of delegation in proposed subsection 9D(14) is overly broad, to the extent it applies to the agency head's power to issue authorisations under proposed subsection 9D(2). While acknowledging the need for flexibility in time-critical circumstances,[41] the Law Council considers that an

[38] Explanatory Memorandum, 14 at [38].

[39] *Acts Interpretation Act 1901* (Cth), section 34AA.

[40] Namely, the decision must have been so unreasonable that no reasonable authority could ever have come to it: *Associated Provincial Picture Houses Limited v Wednesbury Corporation* [1948] 1 KB 223.

[41] Explanatory Memorandum, 58 at [45].

ability to delegate the power to any staff member is disproportionate to the gravity of section 9D authorisations for the following reasons:

- as noted above, the power to grant authorisations under proposed section 9D is effectively a power to confer a wholesale immunity from legal liability upon the persons through whom an agency acts, via the enlivenment of section 14 of the ISA in respect of intrusive intelligence collection activities that would otherwise be illegal under Australian law;
- the factual assessments that must be made under proposed subsection 9D(1) have the potential to be very complex and require the making of intricate value judgments (for example, about the necessity and desirability of collecting intelligence, and determining whether the affected person would have consented to the production of intelligence on them); and
- the conditions in proposed subsection 9D(2) require the person granting the authorisation to stand in the shoes of the responsible Minister for the agency. They must be satisfied not only that the Minister would have been justified in granting the authorisation (that is, it was objectively open to the Minister to grant the authorisation), but also that the Minister would have done so (that is, the Minister would have subjectively exercised their discretion to grant it).

Preferred approach: power to issue section 9D authorisations should be non-delegable

82. The Law Council submits that assessments of the kind listed above involve matters of such gravity and complexity that they require a decision by the agency head personally (which can include an acting agency head).

83. This is particularly the case in respect of conducting an assessment under proposed paragraph 9D(2)(b) to determine whether the responsible Minister would have granted the authorisation request, if it was placed before them for decision. Consistent with the intent of Part 2 of the ISA to place primacy upon Ministerial approval of intrusive intelligence collection in relation to Australian persons, the Law Council submits that any provision which purports to empower an agency official to stand in the shoes of their responsible Minister should be framed in the narrowest possible terms. In particular, such a provision should only confer such power on an agency-level decision-maker who is directly accountable to the responsible Minister; and who has an intimate understanding of that Minister's decision-making approach on authorisation requests, via constant and direct engagement with that Minister across the full breadth of the agency's operational and administrative activities.

84. In particular, the Law Council submits that the ISA agency heads alone possess these characteristics, by reason of their position. The role of agency staff in these circumstances ought to be the provision of advice to the agency head on the granting of an authorisation under proposed section 9D, and not to assume the role of primary decision-maker, as delegates of the agency head's power. Presently, the power to issue emergency agency head authorisations in section 9B of the ISA is not subject to a power of delegation in favour of agency staff. The Law Council submits that a consistent approach should be taken to the new authorisation mechanism in proposed section 9D of the ISA.

85. Accordingly, the Law Council's preferred position is that the power of delegation in proposed subsection 9D(14) should exclude the power to issue authorisations under proposed subsection 9D(2). However, it could include the compliance obligations in relation to record-keeping, notification and reporting under other provisions of that section.

86. The Law Council accepts that the circumstances of urgency which attend hostage, kidnap or mass-casualty type situations occurring outside Australia may create a legitimate need for additional flexibility beyond that found in existing sections 9, 9A

and 9B of the ISA. However, such flexibility should be limited to the devolution of authority from the Minister to the agency head alone (including a person acting as the agency head) with the removal of a requirement for the agency head to first consider whether the relevant Ministers are readily available or contactable (as is presently required by existing section 9B). This devolution of power should not be extended further to staff members of the agency, via a broad power of delegation.

87. The unclassified reports of the Richardson Review and IIR did not appear to specifically address the question of delegation of the new authorisation power. As such, they appeared to countenance the personal exercise of that power by the agency head. Arguably, it is implicit from the global nature of the ISA agencies' functions that the head of that agency will need to be readily available and contactable to deal with matters arising from events outside Australia, and therefore occurring in different time-zones, including in urgent cases. These circumstances should not justify the conferral of a power to delegate primary decision-making responsibility in relation to the granting of an emergency authorisation to engage in intrusive intelligence collection activities.[42]

88. The Law Council acknowledges that ISA agency heads would perform due diligence in making decisions about the exercise of their power of delegation under proposed section 9D(14). The legality and propriety of their decision-making would also be subject to the independent operational oversight of the IGIS. However, these considerations do not displace the need for stronger statutory parameters on the power of delegation itself. Placing reliance on the beneficial exercise of a discretionary power is not a safeguard which guarantees it can only be exercised in a proportionate manner.[43]

89. Similarly, while independent operational oversight is valuable, its *ex post facto* and advisory nature, in relation to the exercise of a broad discretionary power, means it cannot be regarded as a 'substitute' for limiting the scope of the power under primary legislation. In particular, such oversight cannot prevent, or retrospectively invalidate, the improper exercise of that power. Resourcing factors may also mean that it is not possible to conduct individual oversight each time a power of delegation is exercised. It is also conceivable that such oversight may also occur a considerable time after the power has been exercised and the relevant delegates have, in turn, exercised their functions and powers. (For example, oversight might conceivably occur in accordance with periodic inspection cycles, tied to the period of effect of authorisations issued under the ISA.)

Alternative approach: a more limited pool of prospective delegates

90. If the Committee is persuaded that an ISA agency head's power to issue an authorisation under subsection 9D(2) should be delegable to agency staff, then the

[42] Cf Explanatory Memorandum, 58 at [45] which states that the broad power of delegation in relation to the granting of authorisations under subsection 9D(2) is needed to recognise that the ISA agencies 'operate in a range of operational environments, including overseas' and that the power of delegation is needed to ensure that agencies can take swift action. (See further 54 at [19], which emphasises that ISA agencies 'respond to emergencies overseas' and, as such, the requirement for authorisation to produce intelligence 'often arises late at night or in the early hours of the morning in Australia'.) To be clear, the Law Council considers that, while this is a reasonable justification for devolving responsibility for granting emergency authorisations from a Minister to an agency head (and also for relieving the agency head of the obligation in section 9B to consider whether relevant Ministers are readily available or contactable), it is not a sufficient justification for the proposed power of delegation under new subsection 9D(14) in relation to the granting of a subsection 9D authorisation.

[43] Cf Explanatory Memorandum, 58 at [45] which identifies the discretionary nature of the proposed power of delegation as a safeguard, because unlike a statutory power of authorisation, it means that only those staff members who the agency head regards as 'appropriately qualified to make such a significant decision' will be empowered to do so. To be clear, the Law Council's concern is that there are no statutory parameters on the agency head's discretion to make that decision about who is 'appropriately qualified' in the context of the gravity of decision-making about the issuance of authorisations under proposed subsection 9D(2).

Law Council alternatively submits that proposed subsection 9D(14) should be amended to prescribe a narrower class of potential delegates.

91. In particular, the power of delegation should be limited to a class of agency staff members which is defined by reference to their seniority, perhaps in an analogous manner to the concept of a 'senior position-holder' as defined in section 4 of the ASIO Act for the purpose of certain powers of delegation and authorisation under that Act.

92. Defining the class of prospective delegates by reference to their seniority within the agency would provide stronger assurance to the public and Parliament, via primary legislation, that an individual delegate is likely to have the ability to 'stand in the shoes of the Minister' for the purpose of making an assessment under proposed subsection 9D(2); and to fully understand and be accountable for what is effectively a power to confer a legal immunity via the enlivenment of section 14 of the ISA in relation to the acts done pursuant to a section 9D authorisation.

Recommendation 5—power of delegation in ISA subsection 9D(14)

Preferred option

- **The agency head's power of delegation in proposed subsection 9D(14) of the ISA should be amended to exclude the power to issue an emergency authorisation under proposed subsection 9D(2).**

Alternative option

- **If the Committee is persuaded that ISA agency heads should be able to delegate their power to issue authorisations under proposed subsection 9D(2), the power of delegation in proposed subsection 9D(14) should be amended to further limit the class of prospective delegates.**
- **This class should be defined as staff members of the agency (excluding contractors or consultants) who hold a position which is classified as a prescribed level of seniority, potentially in an analogous manner to the definition of a 'senior position holder' in section 4 of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act).**

Schedule 2: Counter-terrorism class authorisations

Key proposed amendments

93. Schedule 2 to the Bill proposes to amend Part 2 of the ISA to expand the circumstances in which an ISA agency can obtain a single MA, which enables it to produce intelligence on all Australian persons falling within a specified class, rather than each MA being confined to the production of intelligence on an individual Australian person.

94. Specifically, the measures in Schedule 2 would enable the issuance of an MA to an ISA agency, which enables it to produce intelligence on all Australian persons who are outside Australia and are, or are likely to be, involved with a listed terrorist organisation which is specified in the instrument of authorisation.[44] That is, the class of Australian persons who may be the targets of an intelligence collection

[44] Bill, Schedule 2, items 2 and 3 (amending sections 8 and 9 of the ISA, to insert the MA requirement in new paragraph 8(1)(iaa) and the new MA issuing grounds in new subsections 9(1AAA) and 9(1AAA) of the ISA).

operation is defined by reference to their involvement with a listed terrorist organisation.

95. This proposed amendment would relieve ISA agencies of the present requirement to obtain multiple, concurrent MAs to produce intelligence on individual Australian persons who are suspected of being involved with a listed terrorist organisation. Rather, a single MA would be issued covering a specified class of persons, and it would fall to the agency (at the point of producing intelligence) to determine whether a particular Australian person is within the class and therefore covered by the MA. This stands in contrast to most of the existing MA grounds under sections 8 and 9 of the ISA, which are limited to authorising the production of intelligence on individual Australian persons.[45]

96. A 'listed terrorist organisation' for the purpose of the new MA ground means an organisation which has been listed as a terrorist organisation pursuant to regulations made under Division 102 of the Criminal Code.[46] The Bill also proposes to partially define the term 'involved with a listed terrorist organisation' for the purpose of the new MA ground. It does so by deeming certain activities involving engagement with a listed terrorist organisation to constitute 'involvement'.[47]

97. Those activities are listed in proposed subsection 9(1AAB) and are expressed as not limiting the circumstances in which a person may be taken to be involved with a listed terrorist organisation. The activities listed in proposed subsection 9(1AAB) cover most of the forms of engagement which are recognised as terrorist organisation offences in Division 102 of the Criminal Code. (Namely direction, membership, participation in training and other activities, recruitment, the provision of financial support, and advocacy for and on behalf of the organisation.)[48]

98. The measures in Schedule 2 would implement a recommendation of the IIR, as endorsed by the Richardson Review, that a class authorisation regime should be available in these circumstances.[49] As the reviews noted, the existing MA grounds under section 9 of the ISA did not meet contemporary needs, given:

- the seriousness of the threat to national security presented by Australian persons who are involved with listed terrorist organisations (such as 'foreign terrorist fighters');
- the number of Australian persons with connections to international terrorist groups; and
- developing threats presented by 'lone wolf' attackers who were previously unknown to authorities, and although not formal members of listed terrorist organisations, were inspired by the ideologies and advocacy of such groups.[50]

99. Consistent with the underlying review recommendations, the Bill further proposes that class MAs issued under the new ground would have a maximum period of

[45] ISA, paragraph 8(1)(a) especially subparagraphs (i), (ii) and (iii). One exception was enacted in 2014, in favour of certain activities of ASIS, which are carried out for the purpose of assisting the Australian Defence Force, in support of overseas military operations. In those circumstances, ASIS may obtain an authorisation to produce intelligence on a class of Australian persons, or to do an act which has a direct effect on a class of Australian persons: ISA, subparagraphs 8(1)(a)(ia) and (ib), as enacted by the *Counter-Terrorism Legislation Amendment Act (No. 1) 2014* (Cth), Schedule 2, item 4.

[46] Ibid, Schedule 2, item 1 (amending section 3 of the ISA to insert a definition of 'listed terrorist organisation').

[47] Ibid, Schedule 2, item 1 (amending section 3 of the ISA to insert a definition of 'involved with a listed terrorist organisation' which has a meaning affected by proposed subsection 9(1AAB) of the ISA, which is inserted by amending item 3).

[48] Ibid, Schedule 2, item 3 (inserting proposed subsection 9(1AAB) of the ISA).

[49] IIR, recommendation 16(a); and Richardson Review, recommendation 45.

[50] Richardson Review, *Unclassified Report, Vol 2*, 121-124 at [20.45]-[20.53]; and IIR, *Unclassified Report*, 97-98 at [6.30]-[6.35].

effect of six months.[51] It would be necessary for the relevant ISA Minister to obtain the agreement of the Attorney-General to the issuance of the MA (consistent with existing requirements for MAs concerning the production of intelligence on Australians who are involved in activities that are likely to be a threat to security).[52]

100. Class MAs issued under the new ground would also be subject to specific record-keeping and reporting requirements.[53] This includes a requirement for ISA agencies to maintain, and make available to the IGIS for inspection, lists of all individual Australians who were determined to be part of the class specified in the MA and upon whom intelligence is intended to be produced in reliance on the MA. They must document the reasons each person was determined to be a class member.[54]

Law Council views

101. The Law Council acknowledges the findings of the IIR and Richardson Review about the necessity of these amendments. It is also supportive of the following attributes of the new class MA ground:

- the limitation of the new class MA ground to Australian persons who are involved with listed terrorist organisations, consistent with the position of the Richardson Review (which endorsed the submissions of the Law Council on this point, cautioning against extension to non-listed organisations);[55]
- the six-month maximum period of effect for class MAs issued under the new ground, and
- the specific reporting and record-keeping requirements in relation to individual Australians who were assessed as being part of the class specified in the MA.

102. In particular, these measures will assist in constraining the breadth of the classes of persons able to be covered by a single MA. The reporting and record-keeping measures are also likely to facilitate independent oversight by the IGIS in relation to agencies' decision-making about whether an Australian person was within the class; and Ministerial visibility and accountability in relation to those matters.

103. However, the Law Council notes that the new class MA ground in proposed subparagraph 8(1)(a)(iaa) will, nonetheless, enable a single MA to authorise the production of intelligence on a large number of individual Australian persons, with such activities attracting immunity from legal liability under section 14 of the ISA. The impact of the proposed amendment is that very significant discretionary authority will be devolved from the responsible Minister for an ISA agency (at the point of deciding whether to issue an MA in relation to an individual) to officials of the relevant ISA agency (at the point of determining whether an individual is within, or outside, the class of persons prescribed in the MA). The broader the class of Australian persons which can be specified in these class MAs, the more extensive the devolution of authority from Ministerial to agency level.

104. In this regard, the Law Council notes that the concept of a person's 'involvement with' a listed terrorist organisation has the potential to be extremely broad, covering

[51] Bill, Schedule 1, item 7 (amending subsection 9(4) of the ISA).

[52] Ibid, Schedule 1, item 3 (inserting new paragraph 9(1AAA)(b) of the ISA). See further the consequential amendments to subsections 9(1AA) and 9(1AB) of the ISA in amending items 4-6.

[53] Ibid, Schedule 1, item 12 (inserting new section 10AA of the ISA) and item 13 (inserting new subsection 10A(3) of the ISA).

[54] Ibid, Schedule 1, item 12 (inserting new subsections 10AA(2)-(4) of the ISA). See also item 13 (inserting new paragraph 10A(3)(b) which requires reports to the Minister on the class MA to include a statement identifying all Australian persons who were identified as being in the class and upon whom intelligence was produced, or was intended to be produced pursuant to the MA).

[55] Richardson Review, *Unclassified Report, Vol 2*, 123 at [20.50] and recommendation 45.

both direct and indirect forms of engagement. The Law Council acknowledges that the issuance and execution of class MAs under the new ground will be subject to the existing safeguards in sections 9-12 of the ISA, which are collectively directed to ensuring the proportionality of activities carried out under an MA.

105. However, given the extensive devolution of authority that is necessarily created by a class-based MA ground and the significance of its consequences (including in enlivening civil and criminal immunities), the Law Council suggests that consideration is given to placing more precise statutory parameters on the concept of 'involvement with' a listed terrorist organisation. This concept could benefit from greater precision in two key respects, which are outlined below.

Possible exhaustive definition of 'involvement with' a listed terrorist organisation

106. The Law Council suggests that consideration is given to making the activities specified in proposed subsection 9(1AAB) an exhaustive definition of the expression 'involvement with a listed terrorist organisation' for the purpose of Part 2 of the ISA.

107. As noted above, proposed subsection 9(1AAB) deems a very broad range of interactions with a listed terrorist organisation to constitute 'involvement with' that organisation for the purpose of the new MA ground, although it does not exhaustively define the concept of involvement for the purpose of Part 2 of the ISA.

108. The Explanatory Memorandum indicates that the non-exhaustive nature of the definition is intended to retain operational flexibility, noting that 'there may be unique situations where, considering all of the facts and circumstances, a person could be involved with a listed terrorist organisation even if their activities do not fall within those listed in subsection 9(1AAB)'.[56]

109. However, the Law Council does not consider that a general appeal to interests in operational flexibility provides sufficient justification for an open-ended definition, having regard to the breadth and significance of the powers conferred under the new class MA ground. (That is, the devolution of authority to agency-level officials to determine whether a person falls within a specified class, and therefore whether intrusive intelligence collection powers can be exercised in relation to them, which attract an immunity from civil and criminal liability under section 14.)

110. The Law Council further notes that the activities which are specified in the inclusive definition of 'involved with' in proposed subsection 9(1AAB) are extremely broad, covering any form of 'participation' in any 'activities' of a listed terrorist organisation.[57] It is therefore difficult to identify a form of interaction with a terrorist organisation which is not capable of being covered by the activities listed in proposed subsection 9(1AAB). The Law Council suggests that the breadth of the matters specified in proposed subsection 9(1AAB) already provide an adequate degree of flexibility.

111. If further activities are presently in contemplation as being capable of constituting 'involvement', they should be specified in this provision. If further types of activities are identified in the future, it would be preferable for a specific case to be made to the Parliament for their inclusion in primary legislation. This would retain the important supervisory and approval role of the legislature, in relation to the conferral and conditions for the exercise of intrusive and covert intelligence collection powers on ISA agencies.

[56] Explanatory Memorandum, 61 at [63].

[57] Bill, Schedule 2, item 3 (inserting proposed paragraph 9(1AAB)(a) of the ISA).

'Support' and 'advocacy' as the basis for 'deemed involvement'

112. The grounds of 'deemed involvement' in paragraphs 9(1AAB)(e) and (f) cover the provision of 'financial or other support' to a listed terrorist organisation, and 'advoca[cy] for, or on behalf of' such an organisation.

113. The Law Council suggests that these grounds are amended to the extent that they apply to non-financial support and advocacy, so that they only cover the provision of non-financial support or advocacy that is material to the organisation's engagement in, or capacity to engage in, terrorism-related activities. (For example, carrying out a terrorist act, or doing acts which are preparatory or ancillary to the commission of a terrorist act.)

114. Otherwise, these grounds of 'deemed involvement' have the potential to cover a range of relatively benign activities. For example, proposed paragraph 9(1AAB)(f) might potentially enable the production of intelligence on Australian lawyers who are retained to make representations to the Minister for Home Affairs for the de-listing of a terrorist organisation, if those lawyers are located outside Australia. Paragraph 9(1AAB)(e) might be capable of covering Australian people who are unable to move from a region which is under the effective governmental control of a listed terrorist organisation; or Australian aid workers who work as neutral 'first responders', providing first aid and critical health care to persons in foreign conflict zones. While it is acknowledged that this is unlikely to be the policy intent, the Law Council supports stronger statutory safeguards to exclude the risk that class-based authorisations could operate in such circumstances.

115. The Law Council notes the statement in the Explanatory Memorandum that proposed subsection 9(1AAB) 'does not specify a minimum quantum of financial support or the level of non-financial support that a person must provide before they may be considered to be "involved with" a listed terrorist organisation'. This reflects an intention that ISA agencies should be able to obtain a class-based MA in order to investigate leads or tip-offs that a person might be involved with a terrorist organisation, where it appears they may be providing a small amount of support.[58]

116. However, the Law Council's concern is not about setting a minimum threshold in respect of the amount of non-financial support that is provided, before a class MA can be issued and intelligence produced on Australians in that class. Rather, the Law Council is calling for greater precision in the purpose to which that non-financial support is directed.[59]

117. The Law Council acknowledges the need for ISA agencies to have the ability to act on initial information which may be very limited (such as by following up leads and tip-offs). However, it does not necessarily follow that this requires the ISA to include a broad and open-ended definition of the expression 'involved with a listed terrorist organisation'. Rather, the anticipatory character of ISA agencies' intelligence collection functions is already clearly reflected in the authorisation criterion in proposed paragraph 9(1AAA)(a). This requires the responsible Minister

[58] Explanatory Memorandum, 61 at [62].

[59] To avoid doubt, the Law Council's comments on these provisions are limited to their coverage of **non-financial support**. The Law Council is not recommending the imposition of a 'materiality' threshold in relation to the provision of financial support to a listed terrorist organisation. This is in recognition that financing a terrorist organisation, in any amount, creates a much higher level of risk, as funds (by their nature) can more readily be pooled and applied to terrorism-related activities. This is consistent with the design of the offence of getting funds to, from or for a terrorist organisation in section 102.6 of the Criminal Code, in which the prosecution is not required to prove that the defendant intended, knew or was reckless as to the particular purpose to which the funds would be put. Rather, the prosecution need only prove the intentional provision of funds, while knowing or reckless as to the circumstance that the group was a terrorist organisation. Cf the offence of providing other support to a terrorist organisation in section 102.7 of the Criminal Code, which imports a materiality threshold. It requires proof that the non-financial support would enable the terrorist organisation to engage in terrorism-related activity; as well as proof of the defendant's criminal fault (that is, knowledge or recklessness) in relation to that circumstance.

to be satisfied that the class of Australian persons specified in the proposed MA is, or is likely to be, involved with a listed terrorist organisation.[60]

Recommendation 6—circumstances in which a person is taken to be 'involved with' a terrorist organisation under proposed ss 9(1AAA) and 9(1AAB)

- **Consideration should be given to exhaustively defining the circumstances in which a person is taken to be 'involved with' a terrorist organisation for the purpose of the class authorisation ground in proposed subsection 9(1AAA). In particular, consideration should be given to transforming the illustrative list of circumstances in proposed subsection 9(1AAB) into an exhaustive definition, noting the significant breadth of those activities.**
- **In any event, consideration should be given to amending the deemed grounds of 'involvement' in proposed paragraphs 9(1AAB)(e) (in relation to 'non-financial support') and (f) (in relation to 'advocacy') so that they only cover the provision of 'non-financial support' to a terrorist organisation, or 'advocacy' for and on behalf of that organisation which is likely to be material to the organisation's engagement in, or capacity to engage in, terrorism-related activities.**

Schedule 3: Class authorisations for ADF support

Key proposed amendments

118. Schedule 3 to the Bill contains a further class authorisation power. It is directed to circumstances in which ISA agencies seek to produce intelligence on Australian persons, for the purpose of providing assistance to the ADF in support of military operations outside Australia, where the Defence Minister has made a written request for that support.

119. Since the enactment of amendments in late 2014, only ASIS has been able to obtain class-based Ministerial authorisations for this purpose.[61] The Bill would expand this to include ASD and AGO. This would implement recommendation 46 of the Richardson Review, which endorsed recommendation 16(b) of the IIR.[62]

Law Council views

120. The Law Council acknowledges that both reviews were satisfied there is a compelling case for the proposed expansion of class authorisations for the purpose of assisting the ADF. They noted that ASIS, ASD and AGO all have statutory functions to render assistance to the ADF in support of overseas military operations, and that all three agencies would therefore face similar issues of efficiency and effectiveness if they were unable to access class authorisations

[60] The inherently anticipatory nature of intelligence collection is also a relevant contextual factor which can be taken into account in the interpretation of all provisions of the ISA which confer functions and powers on ISA agencies. By way of analogy, in *Church of Scientology v Woodward* (1982) 154 CLR 25, the High Court confirmed that the anticipatory nature of ASIO's security intelligence collection functions was relevant to the interpretation of the expression 'intelligence relevant to security' in section 17 of the ASIO Act (which prescribes ASIO's intelligence collection, assessment and advisory functions). Mason J held, at 61, that it will be permissible for even superficial, initial information to be 'checked out and followed up' as part of an intelligence investigation commenced by ASIO (on the basis that it is taken to be 'relevant to security') provided that the initial information is not clearly lacking credibility on its face.

[61] ISA, subparagraph 8(1)(a)(ia), inserted by the *Counter-Terrorism Legislation Amendment Act (No. 1) 2014* (Cth), Schedule 2.

[62] Richardson Review, *Unclassified Report, Vol 2*, 126-127 at [20.61]-[20.63]; IIR, *Unclassified Report,* [6.36].

(namely, the need to obtain multiple, concurrent authorisations as individuals were identified; or an inability to do so in time to produce useful intelligence.)[63]

121. As the Richardson Review noted, there did not appear to be a principled or deliberate reason for the non-inclusion of ASD or AGO in the 2014 amendments enabling ASIS to access class authorisations in respect of its ADF support function. Rather, it appeared that a particular and urgent operational need was identified with respect to ASIS at that time. The Law Council concurs with the reasoning of the Richardson Review that a class authorisation mechanism which is limited to the single function of ISA agencies providing support to the ADF in relation to military operations outside Australia is 'specific and targeted'.[64] It would not enable class authorisations to be granted for intelligence collection 'at large'.

122. Accordingly, the Law Council does not oppose expansion of the class authorisation mechanism with respect to the ADF support functions of ASD and AGO, but recommends further consideration of two matters, as outlined below.

Issues arising from the subsequent use of intelligence by the ADF

123. The provision of intelligence to military operations being conducted outside Australia, particularly in foreign conflict zones, can raise broader issues about Australia's compliance with international humanitarian law. Particular issues may arise in relation to any subsequent uses to which the ADF may put that intelligence—for example, in decision-making about targeting individuals for the use of lethal force—and the extent to which that circumstance was known, or ought to have been the subject of inquiry, at the time an authorisation for the collection of intelligence was sought by, and issued to, the relevant ISA agency.

124. While any subsequent usage of intelligence by the ADF is governed by its Rules of Engagement, and other applicable legal requirements, the Law Council notes that there are, at the very least, issues of propriety arising for intelligence agencies in seeking and executing MAs given under this ground. That is, in considering and informing the Minister as to whether intelligence produced under a proposed MA is, or is likely to be used for, targeting purposes by the ADF, or shared with Australia's allies who may be likely to do so.

125. The proposed expansion of the class authorisation mechanism in Schedule 3 could feasibly result in a 'net expansion' of the scale and pace of intelligence collection activities carried out by ASIS, ASD and AGO for the purpose of assisting the ADF in support of overseas military operations. That is, a single authorisation may authorise the production of intelligence on a broadly defined class comprising large numbers of persons, with decision-making devolved to agency level about whether a prospective intelligence collection target falls within the approved class.

126. The Law Council suggests that the credible possibility of a practical expansion of intelligence collection activities in this context would provide a timely opportunity for the Committee to seek information from relevant ISA agencies about their practices in relation to providing intelligence to the ADF in circumstances which may enable individuals (whether Australians or otherwise) to then be targeted for the use of lethal force.

127. Ideally, unclassified information about contemporary practices to ensure human rights compliance should be placed on the public record, to provide the public and the Parliament with tangible assurances about them. There may also be value in the Committee pursuing this matter in further detail with agencies via classified evidence as needed, and reporting its conclusions to the Parliament.

---

[63] Ibid.
[64] Richardson Review, *Unclassified Report, Vol 2,* 126 at [20.61]-[20.62].

Defence Minister's requests for intelligence agency support

128. Existing paragraph 9(1)(d) of the ISA provides that an 'ADF assistance class MA' can only be issued to ASIS, if (among other conditions) the Defence Minister has made a written request for that assistance. There is currently no maximum period of effect for a request made by the Defence Minister, only the separate MA, if issued. The Bill does not propose to introduce a maximum period of effect for the Defence Minister's request for assistance, as consequential amendment to the expansion of the class MA ground to ASD and AGO.

129. This may mean that an 'ADF assistance class MA' could lawfully be issued to ASIS, ASD or AGO (either anew, or an effective re-issuing of an expired MA after its six-month maximum period of effect) on the strength of a request by the Defence Minister which is some years old, and potentially issued by a previous Minister. Such a request may not accurately reflect the contemporary circumstances surrounding the relevant overseas military operation, and the specific context in which the current assistance is sought.

130. The proposed expansion of the 'ADF assistance class MA ground' to include ASD and AGO (in addition to the existing coverage of ASIS) therefore provides an appropriate opportunity for the inclusion of a statutory maximum period of effect for the Defence Minister's requests for assistance, as an additional safeguard to ensure Ministerial visibility and accountability. This would mean that, for ongoing military operations, the Defence Minister would periodically need to give specific consideration to whether they should make a new request for ASIS, ASD or AGO assistance, and if so, to consider the particular terms of the request at the material time. In particular, the Law Council would support alignment of the maximum period of effect for the Defence Minister's requests with the maximum period of effect for an MA issued to the relevant ISA agency (that is, six months).[65]

Recommendation 7—Maximum period of effect for Defence Minister's requests

- **Paragraph 9(1)(d) of the ISA should be amended to apply a six-month maximum period of effect to written requests made by the Defence Minister for an ISA agency to provide assistance to the ADF in support of military operations outside Australia. (This amendment should apply to ASIS, ASD and AGO.)**

Schedule 4: Altered meaning of 'producing intelligence'

Key proposed amendments

131. Schedule 4 to the Bill proposes to limit the meaning of the expression 'producing intelligence on an Australian person' for the purpose of the requirements in subsection 8(1) of the ISA for agencies to obtain an MA. Its effect will be to reduce the circumstances in which MAs are presently required. (However, the likely practical impacts of that reduction are unclear, in terms of the proportion of agency activities that presently require authorisation under an MA, which will no longer require Ministerial level approval if Schedule 4 to the Bill is enacted. The extrinsic materials to the Bill do not provide an indication of this matter.)

132. Proposed subsection 8(1A) achieves this result by creating the concept of a 'prescribed activity'. It states that an ISA agency will only be taken to be 'producing intelligence on an Australian person' (and therefore required to obtain an MA) if that agency either undertakes a 'prescribed activity' to obtain that intelligence, or expressly or impliedly requests an authority of another country to do so. Proposed

[65] ISA, subsection 9(4).

subsection 8(1B) defines a 'prescribed activity' as a 'covert and intrusive activity' or series of such activities, including those activities for which ASIO would require authorisation under a special powers warrant or a telecommunications interception warrant to carry out in Australia.

133. These amendments purport to implement recommendation 41 of the Richardson Review, which endorsed recommendation 16(d) of the IIR. Both reviews found that the term 'producing intelligence' should be defined in the ISA, to limit the types of activities for which agencies would be required to obtain an MA. In particular, they noted that the ordinary meaning of the term 'producing intelligence' in relation to an Australian person had led to agencies seeking MAs in broader circumstances in which there was no material interference with the privacy or other interests of the persons, and the relevant activities were benign in nature, such as reviewing existing holdings of information or open source materials accessible to the public, or receiving intelligence reporting from foreign partners.[66]

134. The Richardson Review concurred with the IIR that it was not necessary for Ministerial control to be exercised in relation to such activities. Rather, the reviews considered that such control was necessary only in respect of those activities involving conduct that is both covert to the subject, and intrusive to that person's rights or liberties (including privacy). It was envisaged that this would include, but would not necessarily be limited to, the activities for which ASIO would require authority under a warrant to undertake in Australia. (This was in recognition that warrants are generally only required to provide lawful authority for activities that would otherwise constitute a criminal offence; whereas Ministerial authorisation under the ISA is directed to the discrete purpose of ensuring Ministerial control and accountability in relation to those of the ISA agencies' activities which have a significant impact on Australian persons).[67]

Law Council views

135. The Law Council understands the desire to remove requirements to obtain MAs in circumstances in which the relevant activity or activities are self-evidently benign in nature, and would have negligible interference with the rights or liberties of the Australian person or persons being targeted (or other Australian persons).

136. However, as outlined below, the Law Council has identified some aspects of the drafting of proposed subsections 8(1A) and 8(1B) which:

- could unintentionally relieve agencies of the requirement to obtain Ministerial authorisation in broader circumstances than those contemplated by the reviews; or
- may require individual agency staff to make extremely complex and fine distinctions at the point of determining whether to seek an MA, or in assessing whether a proposed activity is supported by an extant MA.

137. In particular, the following matters would benefit from further examination, to ascertain the policy intent in relation to certain activities; and to consider whether amendments may be necessary or desirable to ensure that there is clarity on the face of the legislation:

- implications for the level of authorisation required for geospatial intelligence collection activities by AGO; and
- the application of the 'covert and intrusive' threshold to activities of the following kinds:

[66] IIR, Unclassified Report, [6.42]-[6.43]; and Richardson Review*, Unclassified Report, Vol 2*, 104-105 at [19.116]-[19.124].
[67] Richardson Review, *Unclassified Report, Vol 2,* 104 at [19.117] and 105 at [19.24].

- human intelligence collection, including the use of covert human sources;
- accessing telecommunications data ('metadata'); and
- the interrogation of 'bulk personal datasets' already within an agency's holdings (or the holdings of a partner agency, which is either tasked to interrogate the data sets, or which grants the ISA agency access to the relevant databases).

138. Consideration could be given to adopting a different legislative design approach, more analogous to that in the United Kingdom under section 26 of the *Regulation of Investigatory Powers Act 2000* (UK) (**RIPA**) which provides more detailed statutory guidance on relevant factors in determining whether an activity is 'covert and intrusive'. This matter is also discussed below.

Application to geospatial intelligence collection

139. In all cases, ISA agencies will need to make a factual assessment of whether a particular activity, or series of activities, will meet the threshold of 'covert and intrusive'.

140. In general terms, it seems tolerably clear that the concept of a 'covert and intrusive activity' would cover the offshore collection of certain human intelligence by ASIS. For example, the use of covert human sources who engage with a target, and misrepresent their true identities and motives, in order to extract information from the target, which the target is unlikely to have disclosed voluntarily had they known the true identity of the source, or otherwise have disclosed publicly.

141. It also seems reasonably clear that the collection of certain signals intelligence by ASD would also meet this threshold—for example, the interception of private electronic communications between individuals, such as text messages, emails or audio calls. In both instances, there is active concealment of the agency's activities from the target and others; and the collection methodology is intruding into individuals' rights to privacy, via the extraction or interception of private information.

142. However, it is considerably less clear as to whether many, or possibly most, instances of geospatial intelligence collection could be characterised as being 'covert and intrusive' in relation to an individual Australian person. For example, in the case of acquiring and using satellite imagery, it is conceivable that such imagery will be obtained covertly to the Australian person or persons who are the targets of the intelligence operation. However, that imagery may not necessarily be intrusive to those persons' privacy or other interests, since it may only show geographical features in a designated area, such as buildings or other structures, from a considerable distance. It is conceivable that such imagery, or the act of obtaining it, would not involve the extraction or disclosure of private information.

143. In the result, it is possible that the proposed amendments may substantially reduce the circumstances in which AGO is required to obtain an MA to produce geospatial intelligence on an Australian person. This raises a possibility that a significant proportion of AGO's operations which may currently require Ministerial-level approval would only require internal agency-level approvals. While such a result is not necessarily problematic, the impact on the proportion of agency operations that would no longer require an MA has not been acknowledged in the extrinsic materials to the Bill.

144. If it is correct that the acquisition and use of geospatial intelligence is unlikely, in many instances, to cross the threshold of being 'covert and intrusive', then this outcome would appear to depart from the policy intent underlying the relevant review recommendations to exclude relatively benign activities from Ministerial

authorisation requirements, along the lines of reviewing existing agency holdings or receiving intelligence reports from partners. The Committee may wish to consider this issue further, including an examination of applicable governance arrangements in relation to the approval of geospatial intelligence production activities which presently require an MA, but will no longer be subject to that requirement if Schedule 4 to the Bill is enacted.

Application to human intelligence collection

145. The task of identifying whether certain human intelligence collection activities are 'covert and intrusive' may also be complex and finely balanced. As noted above, it seems clear that the use of a human source would be both covert and intrusive to the target, where that source deliberately concealed their true identity, and cultivated a false relationship with the target for the purpose of extracting information from them, which the target would otherwise have been unlikely to volunteer on a pro-active basis. For example, this might occur if a human source pretended to be a fellow member of an organisation to which the target belonged, or a potential business partner or another associate of the target.

146. However, it is less clear that the activity would be 'covert and intrusive' if a human source simply engaged a target in conversation in a public space, without giving any context about their identity or motivations (for example, exchanging small talk in a queue). It may also be less clear that an MA would be required if a human source simply conducted physical surveillance, by following and observing the target in public places. There may also be some uncertainty in relation to the activities of a source in monitoring a target in 'semi-private' places, such as facilities which are open to the public, but access is subject to membership requirements or other restrictions (for example, the premises of health and recreation or social clubs, or educational or training institutions).

147. Accordingly, it is conceivable that, in practice, there may be scope for considerable latitude in the interpretation of the concept of a 'covert and intrusive activity' in the context of human intelligence collection activities. Neither the Bill nor its extrinsic materials provide guidance about the policy intent in such circumstances.

148. The Law Council suggests that there would be value in the proponents of the Bill publicly explaining the policy intent in relation to whether activities of the kind outlined above would be subject to a requirement to obtain an MA. A clear, unclassified explanation of the policy intent could then be scrutinised by the Parliament and stakeholders, and this could usefully inform an assessment of whether further statutory guidance is needed in relation to the meaning of the expression 'covert and intrusive'.

Application to metadata access

149. Proposed subparagraph 8(1B)(b) provides that, if ASIO is required to obtain an interception warrant under Part 2-2 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) in relation to the interception of a telecommunication in Australia, then the activity is taken to be 'covert and intrusive' if it were to be carried out by an ISA agency for the purpose of producing intelligence on an Australian person.

150. The fact that this provision is limited specifically to telecommunications interception (and not access to telecommunications data, otherwise known as 'metadata' pursuant to authorisations given under Chapter 4 of the TIA Act) could suggest that access to metadata may not be regarded as 'covert and intrusive' in all circumstances.

151. The Law Council notes that the specific reference to telecommunications interception, and the omission of telecommunications data access, may create

uncertainty about the requisite level of authorisation for ASD's activities in acquiring metadata (as a form of signals intelligence) outside the Australian telecommunications network.

152. On one view, access to metadata can be equally, if not more, intrusive to individual privacy than the contents of electronic communications, because of the detailed information that multiple pieces of metadata may reveal about a person's activities, movements and associations (particularly in high volumes over prolonged periods of time). The circumstances in which metadata acquisition will, or will not, be regarded as 'covert and intrusive' are therefore unclear. As with the other types of activities noted above, the Law Council suggests that, as a starting point, there should be clear disclosure of the policy intent in relation to the level of approval required for metadata access.

Application to the interrogation of 'bulk personal datasets'

153. It is also unclear whether the concept of undertaking a 'covert and intrusive activity' would cover the act of an agency interrogating 'bulk personal datasets' within its holdings; or potentially acquiring bulk personal datasets in the first place.

154. The Law Council uses the term 'bulk personal dataset' in this context to denote datasets of personal information about a very large number of individuals, the majority of whom are not persons of interest in an intelligence investigation. Examples include travel-related data such as passenger movement records, records of credit card or other financial transactions, and telephone directories. The individual datasets are held on agencies' electronic intelligence systems, and their contents can be searched collectively by inputting specific selectors, and the results analysed to identify patterns and correlations. The results can be highly intrusive to individual privacy, due to the combination of information returned from numerous, extremely large datasets.

155. It is for this reason that, in the UK, the interrogation of bulk personal datasets must be authorised via warrant issued under Part 7 of the *Investigatory Powers Act 2016* (UK). In contrast, depending on how the expression 'covert and intrusive activity' in the ISA is interpreted, there is a possibility that the proposed amendments to the ISA could have the effect of removing any external, Ministerial approval requirements that may otherwise have applied to Australian intelligence agencies under the ISA in relation to such activities. This would place Australia even further at odds with the warrant-based authorisation system in like-minded jurisdictions in the Five Eyes alliance (which, in addition to requiring external approval, generally involves judicial involvement in that process).

156. Neither the Bill nor the extrinsic materials provide insight in relation to this issue. While the Richardson Review and IIR considered that the activities of agencies in searching existing holdings should not require an MA, those comments did not address the unique circumstances of interrogating bulk datasets. The Law Council similarly considers that there should be a public explanation of the policy intent in relation to the level of approval that an ISA agency would be required to obtain in relation to the interrogation of bulk personal data, if the amendments in Schedule 4 to the Bill were enacted.

Possible statutory guidance on the meaning of 'covert and intrusive' activities

157. The Law Council suggests that a key issue for the Committee in considering the proposed amendments in Schedule 4 is whether there should be greater statutory guidance in relation to the meaning of a 'covert and intrusive' activity, and therefore whether an ISA agency is required to obtain an MA to produce intelligence on an Australian person.

158. As is evident from the above discussion of particular types of intelligence collection activities, an assessment of whether a proposed activity is 'covert and intrusive' is likely to be complex, and has the potential to turn on finely balanced considerations of fact and degree. Accordingly, agency officials may be required to exercise a degree of value judgment in determining whether they are required to obtain an MA. It is possible that reasonable minds may differ as to whether an activity will meet the statutory threshold, with the result that different agencies (and potentially different decision-makers or advisors within agencies) may adopt different interpretive approaches to substantially similar collection activities.

159. The covert and highly classified nature of intelligence agencies' operations makes it unlikely that there will be occasion for judicial interpretation of the expression 'covert and intrusive' in proposed subsection 8(1B) of the ISA. In view of these circumstances, it would be preferable for the statute to provide the maximum degree of clarity possible.

160. This would be compatible with the commentary in the Richardson Review, which observed that intelligence legislation should 'provide clarity where possible'. As that review noted, such clarity is essential to 'support the public to understand the legislation, in turn supporting public trust and confidence in the work of the intelligence agencies'. It also 'provide[s] the agencies themselves with certainty regarding their statutory mandate'.[68] The Law Council is concerned that, as drafted, proposed subsections 8(1A) and 8(1B) of the ISA will not be fully effective in realising these objectives.

161. In this regard, the Law Council notes that, in the UK, section 26 of the RIPA provides more specific guidance on whether an activity is taken to be 'covert' and 'intrusive' for the purpose of the authorisation requirements under Part II of that Act (including in the context of covert human intelligence sources). Consideration might be given to the adoption of similar concepts in the ISA.

162. However, any consideration of the approach taken under the RIPA should also take into account the additional warrant-based requirements under the *Investigatory Powers Act 2016* (UK) under which the UK intelligence services are required to obtain warrants and authorisations for electronic surveillance and other collection activities, including telecommunications interception, access to metadata, interrogating bulk personal data sets, and remote computer access.

163. Relevant factors set out in section 26 of the RIPA include:

- where surveillance 'is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place';[69]
- where surveillance of a person is undertaken 'in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation)'. ('Private information' is defined as being 'any information relating to [a person's] private or family life');[70]
- where surveillance 'is carried out in relation to anything taking place on residential premises or in any private vehicle' (provided that either a person or device is present on the premises or in the vehicle; or a surveillance device is installed off the premises or outside the vehicle, but it provides the same quality and detail of information as a device installed on the premises or vehicle);[71]

[68] Richardson Review, *Unclassified Report, Vol 2*, 104 at [19.121].
[69] RIPA, paragraph 26(9)(a).
[70] Ibid, paragraph 26(2)(b) and subsection 26(10).
[71] Ibid, subsections 26(3) and (5).

- where a human intelligence source 'establishes or maintains a personal or other relationship with a person for the covert purpose of':
  - '[using] such a relationship to obtain information or to provide access to any information to another person; or
  - '[disclosing] information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship'.[72]

Recommendation 8—uncertain meaning of 'covert and intrusive' activities

- **The Government should provide further explanation of the policy intent, in relation to whether the types of activities discussed at paragraphs [137]-[156] of this submission are intended to be characterised as 'covert and intrusive' and therefore subject to the requirement to obtain prior Ministerial authorisation. (That is, geospatial intelligence collection, human intelligence collection including the use of covert human intelligence sources, accessing telecommunications data, and interrogating bulk personal datasets.)**
- **Consideration should be given to amending the Bill to provide further statutory guidance about the meaning of the expression 'covert and intrusive' in proposed subsection 8(1B) of the ISA. This could potentially include some of the relevant factors set out in section 26 of the *Regulation of Investigatory Powers Act 2000* (UK).**

Schedule 5: Extension of ASIS-ASIO cooperative regime

Key proposed amendments

164. The measures in Schedule 5 to the Bill propose to amend the existing regime in section 13B of the ISA, to expand the circumstances in which ASIS may produce intelligence on an Australian person, without obtaining an MA, where this is done for the purpose of cooperating with ASIO. (That is, for the purpose of assisting ASIO to perform its security intelligence functions). Presently, paragraph 13B(1)(b) provides that this cooperative regime is only available where ASIS will undertake the activity, or series of activities, outside Australia.

165. The key proposed amendments, in amending item 1 of Schedule 5, would remove the geographical limitation in paragraph 13B(1)(b). This would make it possible for ASIS to undertake the production of intelligence inside Australia (as well as outside Australia) for the purpose of cooperating with ASIO.

166. Any 'onshore' activities would be subject to equivalent conditions as those for its 'offshore' cooperative activities. Significantly, section 13B cooperative arrangements cannot authorise ASIS to undertake any activity for which ASIO would require a warrant to undertake in Australia, by reason of existing section 13D. Additionally, existing section 13E provides that, in order for ASIS to collect intelligence pursuant to a section 13B cooperative arrangement, its Director-General must be satisfied that there are satisfactory arrangements in place to ensure that the relevant activities will be limited to those which are necessary and proportionate to the purpose of assisting ASIO.

Rejection of Richardson Review recommendation

167. The proposal to repeal the geographic limitation in existing paragraph 13B(1)(b) of the ISA is controversial. While the IIR supported that proposal, the Richardson Review subsequently opposed it, and rejected the reasoning given by the IIR. The

[72] Ibid, subsection 26(8) and paragraphs 26(9)(b) and (c).

Richardson Review commented that legislative amendment was not necessary or proportionate to address practical issues raised by agencies about inefficiencies and delays in making arrangements for inter-agency cooperation, particularly with respect to onshore intelligence collection:

> *There is insufficient evidence before the Review to demonstrate the operational need for such a supporting role onshore in the same way as it is needed offshore. The Review considers that any [practical] issues with the 13B regime can be mitigated by focusing on collaboration, understanding and working relationships between ASIO and ASIS staff, at all levels.*[73]

168. The Law Council notes that the reasoning of the Richardson Review appeared considerably more detailed than the commentary documented in the unclassified IIR report, which presented a conclusion that the geographical restriction in section 13B was an impediment to cooperation, without supporting justification (although it is possible that the classified version of the IIR report may have contained detailed explanation).[74]

169. The Law Council notes that the Explanatory Memorandum to the Bill restates the conclusion in the IIR report, that 'the current geographic limit restricts cooperation that is essential to thwarting attacks in defeating other threats to security' including because 'as Australia's security environment becomes more complex … the lines of demarcation between security and foreign intelligence [become] more porous'.[75]

170. However, the Explanatory Memorandum does not clearly explain why it is necessary to adopt the specific form and mechanism of cooperation proposed in Schedule 5, in order for agencies to operate effectively in this environment. (That is, a framework under which ASIS operates domestically, on the request of ASIO, to produce intelligence on Australian persons, in the absence of a requirement for Ministerial approval.) The extrinsic materials to the Bill do not clearly identify why it is not possible to achieve the same result by taking the practical steps supported by the Richardson Review, to enhance the efficiency and effectiveness of inter-agency cooperation under existing statutory frameworks.

Law Council views

171. Given the conclusions of the Richardson Review that there was insufficient evidence of a need for the form of legislative intervention now proposed in Schedule 5 to the Bill, the Law Council urges caution in scrutinising the case for the necessity of these proposals.

Necessity of extending the scheme to domestic collection

172. The Law Council considers that the limited justification offered in the extrinsic materials to the Bill does not establish the necessity of the proposed removal of the geographic limitation on section 13B cooperation between ASIS and ASIO. The Law Council would not support the enactment of the measures in Schedule 5 unless compelling evidence of their necessity is provided.

Utility of existing cooperative mechanisms under the ASIO Act

173. In particular, no explanation is given as to why it would not be practicable for ASIO to simply avail itself of its existing powers to authorise ASIS staff members, among other persons, to exercise authority under ASIO's own warrants and other operational authorities, in accordance with existing provisions of the ASIO Act.

---

[73] Richardson Review, *Unclassified Report, Vol 2,* 163-164 at [22.65] and recommendation 57.
[74] IIR, *Unclassified Report*, [5.59] and [6.61].
[75] Explanatory Memorandum, 25 at [103] and 26 at [206].

(For example, the power in section 24 to authorise persons to exercise authority under one of ASIO's special powers warrants; or the exercise by the Director-General of their powers as an employer under Part V of the ASIO Act to second staff members of ASIS where their expertise is needed.)

174. Pursuing these arrangements under existing provisions of the ASIO Act would have the effect of making those individual ASIS staff members 'ASIO affiliates' under section 4 of the ASIO Act—effectively, secondees to ASIO, who are performing functions for and on behalf of ASIO, and are subject to the direction, supervision and control of the Director-General of Security in respect of those activities.

175. Neither the Bill nor the extrinsic materials address why a new cooperative scheme is required, under which ASIS performs activities within Australia in support of ASIO, at ASIO's request, but in its own legal capacity as ASIS, with its own separate operational command and governance arrangements to those of ASIO.

176. The fact that two human intelligence collection agencies would be able to operate domestically, in respect of the same security intelligence matters, could create a risk of conflict, inconsistency or lack of coordination between the respective approaches of ASIO and ASIS to the same or similar collection exercises. The Law Council considers that existence of this risk is material to an assessment of the necessity of the proposed measure. It is not merely a practical consideration which can be left solely to the implementation of administrative arrangements.

177. The Law Council acknowledges that new subsection 13(3) of the ISA (amending item 2 of Schedule 5 to the Bill) will provide that ASIS can only undertake domestic intelligence collection activities pursuant to a section 13B arrangement if it has been requested by ASIO. (The limited exception in existing paragraph 13(1)(d) will only allow ASIS to proceed without a prior request from ASIO in circumstances of urgency, where the relevant intelligence collection is carried out overseas.)

178. This is welcome to ensure ASIO has overall visibility and control in relation to domestic collection activities undertaken by ASIS for the purpose of assisting ASIO. However, it does not alleviate the Law Council's concern about the risk of inconsistency, conflict or lack of coordination. The Law Council is concerned about such risks arising at the 'granular' level of individual intelligence collection activities by individual officers, in reliance upon a request from ASIO.

179. It is conceivable that a request furnished by ASIO under paragraph 13B(1)(d) of the ISA may be framed in broader terms, seeking more general assistance in collecting intelligence inside Australia about an identified security threat or foreign intelligence matter (such as an individual, organisation or body politic). It may not necessarily prescribe the particular intelligence collection activities to be carried out, or how they should be carried out. (While it would arguably be open to ASIO to issue requests in these more specific terms, paragraph 13B(1)(d) of the ISA does not require this, as it refers to the Director-General of Security notifying ASIS that 'ASIO requires the production of intelligence on the Australian person or class of Australian persons'.)

180. In contrast, the risks identified by the Law Council could be managed more effectively if individual ASIS staff were effectively 'seconded' to ASIO (as 'ASIO affiliates'). In this legal capacity, they would be performing the intelligence collection activities for and on behalf of ASIO, and would be included directly in ASIO's chain of command, rather than acting for and on behalf of ASIS.

Anomalies with approval requirements for ASIO's foreign intelligence collection

181. Moreover, the proposed expansion of section 13B to 'onshore' cooperative activities by ASIS, without the need for Ministerial approval, is at odds with the

statutory requirements in the ASIO Act governing the converse situation. That is, where ASIO seeks to collect intelligence inside Australia, which is 'foreign intelligence' (being intelligence about the capabilities, activities, and intentions of persons or organisations outside Australia)[76] rather than 'security intelligence' (being intelligence that is relevant to specified threats to Australia and Australians, from which there is a need for protection).[77]

182. In these circumstances, section 27B of the ASIO Act provides that ASIO must obtain the approval of the Attorney-General (who is required to consult with the Foreign Minister or Defence Minister, or both, as applicable). This approval is required notwithstanding that the relevant foreign intelligence collection activities sought to be undertaken inside Australia would not involve the exercise by ASIO of warrant-based powers (that is, because the relevant activities would not otherwise constitute an offence).

183. Examples of foreign intelligence collection activities that would require Ministerial approval under section 27B of the ASIO Act could include deploying a human source to engage with the target in a public place within Australia, or to physically observe their activities in public within Australia. These would appear to be the types of activities that ASIS would likely perform inside Australia, in support of ASIO's performance of its functions, including the collection of security intelligence, if Schedule 5 were passed. (This reflects the prohibition in section 13D of the ISA, which means that ASIS could not rely on a section 13B cooperative arrangement with ASIO to undertake intelligence collection activities for which ASIO would need a warrant to undertake in Australia.)

184. The Committee may wish to explore this apparent anomaly in the respective requirements for Ministerial involvement, where ASIO is collecting foreign intelligence in Australia (under section 27B of the ASIO Act) and where ASIS is collecting security intelligence in Australia (under section 13B of the ISA).

Recommendation 9—further information about the necessity and implications of the proposed repeal of paragraph 13B(1)(b) of the ISA

- **Further information should be provided about the necessity of the proposal to enable ASIS to undertake domestic intelligence collection under section 13B of the ISA. It should address the following matters:**
  - **the reasons that it is not considered practicable for ASIO to utilise the operational assistance of individual ASIS staff members as secondees to ASIO ('ASIO affiliates'), and why ASIS should be permitted to collect domestic intelligence in its own, separate legal capacity to ASIO (with separate operational command and governance arrangements);**
  - **how risks of overlap, conflict, inconsistency or lack of coordination—which may arise from two intelligence agencies**

[76] ASIO Act, section 4 (definition of 'foreign intelligence'). See also paragraph 17(1)(e) which prescribes ASIOs more limited statutory function in relation to the collection in Australia of foreign intelligence. While there is some overlap with security intelligence (intelligence relevant to 'security' as that term is defined in the ASIO Act) the key difference is that security intelligence requires the existence of a threat to Australia or its people, from which there is a need for protection. Foreign intelligence is not directed only to circumstances in which there is an identified threat to security or other national interests.

[77] ASIO Act, section 4 (definition of 'security'). The threats covered by the definition of security are broad, including espionage, sabotage, foreign interference, attacks on Australia's defence system, the promotion of communal violence, politically motivated violence, and serious threats to Australis's territorial and border integrity. The definition also includes fulfilling Australia's obligations to other countries in relation to these matters. See also, paragraph 17(1)(a) which prescribes ASIO's collection function in relation to security intelligence (expressed as 'intelligence relevant to security').

operating domestically to collect the same kinds of intelligence—will be managed in practice; and

- **why there is no Ministerial involvement in the approval process for ASIS to collect domestic security intelligence in support of ASIO under section 13B of the ISA (as amended); notwithstanding that ASIO requires ministerial approval under section 27B of the ASIO Act to collect foreign intelligence in Australia (even though the collection activities do not require authorisation under a warrant).**

Schedule 8: Timeframe for suspension of travel documents

Key proposed amendments

185. Schedule 8 to the Bill deals with matters that were not the subject of recommendations in the IIR or Richardson Review. It proposes to amend the regimes in section 22A of the *Australian Passports Act 2005* (Cth) and sections 15A and 16A of the *Foreign Passports (Law Enforcement and Security Act) 2005* (Cth) for the temporary surrender of Australian passports or foreign travel documents on security-related grounds.

186. Presently, these regimes allow for the temporary suspension or temporary surrender of such documents for a maximum period of 14 days, during which time ASIO may complete a security assessment in relation to the person (noting that the furnishing by ASIO of an adverse security assessment is a condition precedent to the exercise of the substantive power of cancellation of the relevant travel documents). The Bill proposes to extend the maximum suspension period from 14 days to 28 days.

187. The Explanatory Memorandum states that the current maximum period of 14 days provides insufficient time for ASIO to complete the intelligence collection and analytical process required to furnish the relevant security assessment. It states that operational experience has indicated there has been 'a marked increase in the complexity and volume of matters under consideration' including persons seeking to travel overseas to fight with, or support, terrorist organisations.[78] It notes that there have been circumstances of considerable urgency, in which the first time a person comes to ASIO's attention is when they are preparing for an imminent departure from Australia to a foreign conflict zone.[79] It further indicates that an extended period of 28 days will also alleviate any need for ASIO to 'divert resources from other priority investigations' in order to meet the 14-day timeframe.[80]

Law Council views

188. The Law Council acknowledges the significant urgency and complexity in which ASIO is required to furnish security assessments in relation to the cancellation of Australian or foreign travel documents on security related grounds. It does not oppose, in principle, the proposed doubling of the statutory timeframe. However, the Law Council considers that insufficient justification has been placed on the public record to demonstrate the necessity of the proposed amendments.

189. The Law Council encourages the Committee to explore, in classified evidence as necessary, the specific causes of the administrative impost upon ASIO that is

[78] Explanatory Memorandum, 31 at [143].
[79] Ibid, 31 at [145].
[80] Ibid, 32 at [147].

noted in the Explanatory Memorandum. The Law Council urges caution in extending maximum periods of suspension for travel documents (and thereby limiting human rights, particularly the right to freedom of movement) primarily on the basis of administrative considerations for administering agencies.

190. The significance of the proposed doubling of the temporary suspension period is reflected in the fact that the first Independent National Security Legislation Monitor, Bret Walker SC, supported a temporary suspension power with an indicative maximum period of effect of seven days (in 48 hour increments)—which would be quadrupled if Schedule 8 to the Bill were enacted.[81] The (then) INSLM acknowledged that timeframes could be 'somewhat arbitrary' and the precise timeframe would require further consideration, including in consultation with ASIO and civil society stakeholders. However, the underlying principle was that the power to temporarily suspend a travel document should be subject to a 'strict timeframe' to reflect that the formal furnishing by ASIO of an adverse security assessment would not be a condition precedent to the initial, temporary suspension.[82] This tends in further support of any proposed extension of the maximum period of suspension being supported by compelling evidence of its necessity, to the exclusion of mere convenience or enhanced efficiency alone.

191. The Law Council therefore suggests that careful consideration is given to whether amending the statutory maximum timeframe to effectively accommodate present matters of internal agency administration and workload is the appropriate solution, at least in the absence of evidence suggesting that there have been attempts to implement administrative measures to improve efficiency. (For example, by increasing resourcing, or changing resource allocation priorities to meet the existing, 14-day deadline.) Ideally, administrative solutions should be considered and excluded, if not attempted and assessed to be insufficient, before the permanent legislative doubling of the maximum suspension timeframe is pursued.

Recommendation 10—necessity of proposed doubling of suspension timeframe

- **Further information should be provided about the necessity of the proposal to double the maximum period of interim suspension of Australian or foreign travel documents.**
- **In particular, further information should be provided as to why a permanent doubling of the statutory maximum period of effect is needed in preference to taking administrative action (such as increasing and re-prioritising resources) in order to meet the 14-day time period. This should include explanation of why any spike in current caseload is anticipated to be ongoing or sufficiently long-term as to justify statutory intervention (which will last indefinitely).**
- **While it may be necessary for the Committee to obtain such evidence in camera, by reason of its classified nature, consideration should be given to placing on the public record as much additional information as possible about the necessity of the proposed amendments, as distinct to gains in convenience or efficiency.**

Schedule 9: Expanded immunities for computer-related acts

Key proposed amendments: immunities for ASIS and AGO staff

192. Schedule 9 to the Bill proposes to expand the criminal and civil immunities for ASIS and AGO staff members in Division 476 of the Criminal Code for certain computer-related activities which occur inside Australia, but were intended to occur

[81] Bret Walker SC, INSLM, *Unclassified Annual Report 2014*, (28 March 2014), 48.
[82] Ibid.

outside Australia. (This scenario may eventuate because it was impossible for the agency to accurately locate the computer being targeted due to the use of geolocation blocking technology by the target, but it was reasonably believed that the relevant computer was located outside Australia.)

193. The computer-related activities covered by the Division 476 immunity principally comprise conduct which would constitute a computer offence in Part 10.7 of the Criminal Code. This includes unauthorised access to or modification of data held in a computer; unauthorised impairment of electronic communications to and from a computer; or unauthorised impairment of the reliability, security or integrity of electronic data held on a computer or peripheral device.

194. The immunity also extends to civil liability (such as the tort of negligence) in recognition that individuals who are reliant on computers whose functioning is impaired might seek compensation for any loss or damage they may sustain as a result of being unable to conduct business or personal affairs using that computer. As such, the proposed immunity would extinguish the legal rights of individuals to compensation in respect of property damage or pure economic loss (such as loss of income).

Recent amendments in relation to ASD immunities

195. Recently, Schedule 2 to the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) extended the immunity in this way for ASD staff. The Bill proposes to extend it for staff members of ASIS and AGO. This is consistent with recommendation 74 of the Richardson Review, which supported the expanded immunity for staff members of all three ISA Act agencies, in recognition of evidence from agencies that it can be technically impossible to accurately identify the geographical location of a computer, including due to geolocation blocking technology and the physical portability of computers across jurisdictional boundaries. The Richardson Review considered that retaining the historical limitation of the immunity to computer-related acts done outside Australia may leave ISA staff members exposed to liability. It noted that the risk, or perceived risk, of exposure to liability may limit their willingness to undertake activities which are important to Australia's national security and other interests.[83]

Law Council views

196. The Law Council made submissions to the Committee in relation to the proposed expansion of the immunity in favour of ASD, as part of the inquiry into the SOCI Bill.[84] These submissions are also the position of the Law Council in relation to the proposed expansion of the immunity to ASIS and AGO staff members.

197. In summary, while the Law Council did not categorically oppose the extension of the immunity to the relevant computer-related acts occurring within Australia, it raised questions about its necessity, in particular as to why an immunity was needed in preference to placing reliance on the defence of mistake of fact in relation to the geographical location of a computer (with respect to the potential exposure of agency staff members to prosecution for computer-related offences).

198. The Law Council also raised questions about the broader implications of the expanded immunity. This included whether it should encompass an immunity from civil liability, or be limited to criminal liability. (Noting that the expansion of the immunity to acts done inside Australia will increase the prospect of causing

[83] Richardson Review, *Unclassified Report, Volume 2*, 226-227 at [24.200]-[24.203].

[84] Law Council of Australia, *Submission to the PJCIS Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020*, (February 2021), 97-106.

significant loss or damage to Australian persons. It will extinguish the rights of affected Australians to obtain a legal remedy in respect of that loss or damage.)

199. The Law Council also queried whether aspects of the technical drafting of the immunity provision may be unintentionally broad, in that they might potentially operate to confer immunity for any telecommunications interception or access to telecommunications data, which may occur as part of the technical process of gaining access to data that is held in, or is accessible from, in a computer.

200. The Committee recommended that further consideration be given to the issues raised in the Law Council submission, as follows:

> *[T]he Committee is recommending that Schedule 2 of the SOCI Bill be reviewed with the concerns expressed by the Law Council of Australia in mind, and amended … taking into account the following principles:*
>
> - *whether an immunity, rather than a defence of a mistake or ignorance of fact, is a more suitable mechanism to address potential accidental onshore acts. If so, articulate the preference in explanatory material;*
> - *whether the proposed immunities are appropriate to extend to both criminal and civil liabilities, given the proposed expanded civil immunity leaves no recourse for affected entities to seek reparations for unintended damages;*
> - *whether the expanded immunity could adversely 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).*[85]

201. This recommendation was outstanding at the time of writing the present submission. The Law Council supports its implementation in relation to the expansion of the immunity for ASD as in force, and the proposed expansion for ASIS and AGO in Schedule 9 to the present Bill.

Recommendation 11—implementation of the Committee's recommendation 10 on the SOCI Bill, in relation to ASD, ASIS and AGO

- **The Government should implement recommendation 10 in the Committee's advisory report on the SOCI Bill, in relation to the expansion of the immunity in favour of ASD staff members, and the proposed expansion in favour of ASIS and AGO staff members.**

General comments on Schedules 6-7 and 10-14

Schedule 6: AGO cooperating with 'authorities of other countries'

Key proposed amendments

202. Schedule 6 proposes to amend section 13 of the ISA to modify the requirements governing AGO's cooperation with authorities of other countries. Currently, paragraph 13(1)(c) only permits ISA agencies, including AGO, to cooperate with authorities of other countries if the responsible Minister has given prior approval.

[85] PJCIS, *Advisory Report on the SOCI Bill*, (September 2021), [3.62] and recommendation 10.

203. Schedule 6 proposes to insert new subsection 13(3A), which would effectively create an exception for AGO where that agency is performing certain of its non-intelligence collection functions. (This includes in directly providing imagery or other geospatial, hydrographic, meteorological or oceanographic products, provided that they are not intelligence obtained in the performance of AGO's separate collection functions; or assisting in the production and use of such products or technologies.)[86]

204. In these circumstances, AGO would not be required to obtain the prior approval of the Defence Minister to intended instances of cooperation with foreign authorities. Rather, new subsection 13(3B) would require the Director of AGO to furnish retrospective annual reports to the Defence Minister providing details of 'significant' cooperation.

205. The Explanatory Memorandum to the Bill notes that the measures have been included for efficiency reasons given the volume of cooperation; and on the basis of an assessment that the relevant functions of AGO which would be exempt from the approval framework are 'non-intelligence functions and do not involve covert or intrusive activities'.[87] For the latter reason, it is also suggested that the proposed amendments do not engage any human rights.[88] It is further suggested that the underlying policy intent of the prior Ministerial approval condition in existing paragraph 13(1)(c) is directed to 'typically higher risk activities, involving politically sensitive, covert or intrusive intelligence capabilities'.[89]

Law Council views

206. The Law Council supports the requirement in proposed subsection 13(3B) that AGO must report to the Defence Minister and IGIS about 'significant' forms of cooperation. This is valuable in ensuring Ministerial visibility, control and accountability in relation to such cooperation, in lieu of the removal of the approval requirement for certain of AGO's cooperative activities.

207. However, the concept of 'significance' in relation to such cooperation may be open to different interpretations. The proposed amendments could import a degree of subjectivity, in that they are likely to involve the exercise of value judgment about whether a particular form of cooperation crosses the threshold of 'significance' and is therefore subject to Ministerial reporting requirements.

208. As reports on such cooperation are likely to be classified and would therefore not be the subject of public knowledge, the Law Council is particularly concerned to ensure that human rights considerations are routinely integrated into decision-making by AGO about the 'significance' of cooperation with foreign authorities.

209. Even where the relevant assistance is not the direct sharing of intelligence or the provision of intelligence collection capabilities, but rather other forms of technical information or capability assistance, it is important that careful consideration is given to the human rights record of the government of the other country, and that a balancing exercise is undertaken. It is essential that risk assessments are undertaken in relation to all proposed cooperation, in relation to whether the provision of information or technical capability or other technical support to the foreign authority may enable the other country to engage in activities that are

[86] ISA, paragraph 6B(1)(e). The proposed amendments in Schedule 6 would also relieve AGO of the requirement to obtain prior Ministerial approval of cooperation with foreign authorities in the course of AGO performing its functions in paragraph 6B(1)(ea) (provision of assistance in relation to emergency response, safety, scientific research, economic development, cultural and environmental protection functions); and paragraph 6B(1)(h) (maritime safety functions, such as the provision of nautical maps and surveys).

[87] Explanatory Memorandum, 28, [119].

[88] Ibid, [123].

[89] Ibid, [121].

incompatible with Australia's human rights. A prior approval mechanism outside the agency, namely via its Minister, could feasibly create a strong incentive for thorough due diligence and the documentation of reasoning in relation to these matters.

210. Consequently, the potential human rights risks that could arise in the absence of a requirement to obtain Ministerial approval of proposed cooperation will arguably place an even greater degree of importance on the independent operational oversight of the IGIS. It would be within the functions of the IGIS to conduct oversight not only of AGO's actual cooperation with foreign authorities, but also of the agency's assessment of whether a particular form of cooperation is 'significant' and therefore enlivens the obligation to report to the Defence Minister. Oversight of the latter could include AGO's operational decision-making framework and policies on cooperation in the abstract, as well as their implementation to specific cooperative activities.

211. The Law Council makes no specific recommendations about this matter. However, it notes that the Committee may wish to make inquiries of AGO about its supporting governance framework for assessing whether cooperation with a foreign authority is 'significant', particularly in the context of assessing any risk that AGO's cooperation may enable the government of the foreign country (or the governments of other countries) to engage in human rights violations. The Committee may also wish to consider recommending revision of the human rights statement of compatibility in the Explanatory Memorandum to the Bill to specifically address this matter, noting the suggestion in the present version that the measures in Schedule 6 do not engage any human rights.

212. Existing subsections 13(4)-(6) of the ISA contain similar provisions to those proposed for AGO in Schedule 6, which exclude ASD from the prior Ministerial approval requirement in paragraph 13(1)(c) with respect to some of its non-intelligence functions. The Committee may therefore wish to seek information from ASD about its approach to the interpretation of 'significant' cooperation for the purposes of its Ministerial reporting functions, and potentially engage with the IGIS about this matter. This might include examination of ASD's decision-making and governance framework concerning potential human rights risks.

Schedule 7: ONI cooperating with other entities

Key proposed amendments

213. Schedule 7 to the Bill proposes to amend the *Office of National Intelligence Act 2018* (Cth) (**ONI Act**) to address an apparent oversight in the drafting of the original provisions of section 13 dealing with cooperation between ONI and other bodies, including foreign governments. The provisions generally require ONI to obtain the prior approval of the agency head, the Director-General of National Intelligence (**DG-NI**), before cooperating with authorities of foreign governments. The DG-NI must then notify the Prime Minister, as the relevant portfolio minister, of such cooperation on a monthly basis. The Prime Minister has a power to cancel an approval given by the DG-NI.

214. The term 'authority of another country' is undefined in the ONI Act. However, the Explanatory Memorandum to the Bill indicates that the term is not considered capable of extending to 'public international organisations' such as organs of the United Nations, or other bilateral or multilateral bodies performing 'governmental-type' functions under international law. On this basis, the Bill proposes to expand the requirement in section 13 to obtain prior DG-NI approval for cooperation with a 'public international organisation' as defined in section 70.1 of the Criminal Code. This definition effectively covers an organisation whose membership comprises

two or more countries; or a subsidiary body of such an organisation such as a discrete office, commission, council or committee.

Law Council views

215. The Law Council supports the inclusion of this additional safeguard, as a statutory pre-condition to ONI's cooperation with foreign governmental entities (however described in legislation). The activities and status of public international organisations are more akin to those of domestic governmental bodies than private organisations. Accordingly, it is preferable that the statutory approval requirements for cooperation between ONI and public international bodies are aligned with those applying to cooperation between ONI and authorities of foreign governments.

Schedule 10: Statutory privacy rules

Amendments to the ISA

Key proposed amendments

216. Parts 1 and 2 of Schedule 10 to the Bill propose to implement recommendation 189 of the Richardson Review, which supported a consistent statutory basis for the making and adherence to privacy rules governing the activities of ASIS, ASD, AGO and DIO in retaining and communicating intelligence concerning Australian citizens and residents. These rules are made by the relevant responsible Minister for each agency. They are significant because intelligence agencies are exempt from the requirements of the *Privacy Act 1988* (Cth) (**Privacy Act**) in relation to personal information. However, the Richardson Review identified some anomalies in the legal basis for the making and public disclosure of ISA agencies' privacy rules.[90]

217. In particular, section 15 of the ISA only mandates the making of privacy rules in relation to ASIS, ASD and AGO. It does not cover DIO, whose privacy rules are presently made on an administrative basis. Moreover, subsection 15(7) of the ISA provides that the privacy rules are not legislative instruments and does not otherwise oblige the agencies or their Ministers to publish the rules, including as they are amended from time-to-time—although, in practice, most agencies publish their rules on their respective websites. Further, section 15 of the ISA does not contain an explicit obligation which provides that the ISA agencies must adhere to the privacy rules in their communication of intelligence on Australian persons.[91] The measures in Parts 1 and 2 of Schedule 10 will rectify these issues, in line with recommendation 189 of the Richardson Review.

Law Council views

218. The Law Council is supportive of these measures and has no substantive concerns with their drafting or design. Placing these rules on a consistent statutory footing—including the imposition of explicit obligations to make them publicly available on agency websites, and the imposition of an express statutory obligation on agencies to adhere to those rules—will strongly convey their importance. It will also promote transparency to the public and the Parliament about the substantive requirements in the rules.

219. As a matter of administrative practice, the Law Council would also support consultation with civil society on the review and proposed amendment of those rules, to the greatest extent consistent with security requirements. The Law

[90] Richardson Review, *Unclassified Report, Vol 4*, 50-51 at [43.170] and [43.173]-[43.174].

[91] Subsection 15(1) is expressed as imposing an obligation on the relevant Minister to make rules in respect of their agencies. However, a corresponding duty to adhere to them could be implied from one or both of the provisions of section 15 of the ISA, or the provisions of Part 2-2 of the *Public Governance, Performance and Accountability Act 2013* (Cth) imposing obligations on Commonwealth agency heads and officials.

Council has previously called for similar periodic review and consultation in relation to the ASIO Guidelines, made by the Minister for Home Affairs under section 8A of the ASIO Act, which are administratively binding on ASIO in the performance of its functions (including the handling of intelligence comprising or including personal information on Australians).[92] Consideration could be given to including periodic review and associated consultation provisions in ISA agencies' privacy rules.

Amendments to the ONI Act

220. Part 3 of Schedule 10 proposes several amendments to existing provisions of section 53 of the ONI Act, which prescribe the requirements for the making and content of privacy rules governing ONI's activities in the collection, handling, retention and communication of personal information about Australian persons (noting that ONI is also exempt from the Privacy Act).

Amendments implementing Richardson Review recommendation 12

221. The key amendments would implement recommendation 12 of the Richardson Review, which supported narrowing the scope of ONI's privacy rules in relation to information the agency had obtained in the course of performing its 'open source' intelligence function in paragraph 7(1)(g) of the ONI Act. (That is, 'to collect, interpret and disseminate information relating to matters of political, strategic or economic significance to Australia that is accessible to any section of the public'.) The Richardson Review recommended that the privacy rules in relation to the communication of information obtained by ONI in the performance of its 'open source' function should only apply where ONI had applied its own analysis (and not the 'raw information' itself). This was on the basis that the 'raw information' obtained by ONI was already publicly accessible, and the privacy risk arising from subsequent disclosure by ONI was consequently low. In the result, the compliance burden was disproportionate to the benefit in protecting personal privacy.

222. The Law Council has no substantive concern with the recommendation or reasoning of the Richardson Review on this point, or those of the proposed amendments in Part 3 of Schedule 10 to the Bill which propose to implement that recommendation.[93] The Law Council notes that the privacy rules would still be required to govern the collection by ONI of personal information in relation to an Australian person in the course of performing its 'open source' intelligence function. Only the subsequent communication of that 'raw information' would be excluded from the scope of the regulatory requirements in the privacy rules.[94]

Additional amendments

223. Part 3 of Schedule 10 proposes additional limitations on the scope of ONI's privacy rules in relation to the communication of personal information about Australian persons. These additional limitations were not recommended by the Richardson Review, which was confined to personal information obtained in the course of ONI performing its 'open source' function in paragraph 7(1)(g) of the ONI Act.

---

[92] See, for example, Law Council of Australia, *Comments on the Minister's Guidelines to ASIO*, August 2020, 16-18 at [45]-[55]; and Law Council of Australia, *Submission to the PJCIS review of the Australian Security Intelligence Organisation Amendment Bill 2020*, (July 2020), 95-96 at [403]-[409].

[93] Bill, Schedule 10, item 23 (inserting new subsections 23(1A)-(1C) of the ONI Act, to the extent that these provisions apply to information obtained by ONI in the course of performing its 'open source' intelligence analysis functions under paragraph 7(1)(g) of the ONI Act).

[94] Ibid. Proposed paragraph 53(1A)(a) of the ONI Act applies explicitly to the collection of 'personal information' (defined in proposed subsection 53(1B) in a manner consistent with the definition in the Privacy Act). Proposed paragraph 53(1A)(b) of the ONI Act only applies to the communication of 'intelligence information that is personal information'. Proposed subsection 53(1C) defines 'intelligence information' to comprise 'intelligence' that is produced by ONI in the course of performing its open source function in paragraph 7(1)(g) of the ONI Act (among other analytical functions, as discussed subsequently in this submission).

224. The additional limitations would effectively provide that the privacy rules need only regulate the communication of personal information which ONI has obtained in the course of performing its other two 'analytical' functions (contained in paragraphs 7(1)(c) and (d) of the ONI Act) if ONI has applied its own evaluation or analysis to that 'raw information' it has obtained. It would similarly exclude the mere communication by ONI of 'raw information'.[95]

225. The analytical functions in paragraphs 7(1)(c) and (d) of the ONI Act cover the provision of strategic assessments in accordance with the Government's requirements, in relation to international matters, and domestic matters where incidental to the performance by ONI of other functions. Namely:

> *(c) to:*
>
> *(i) assemble, correlate and analyse information relating to international matters that are of political, strategic or economic significance to Australia, including domestic aspects relating to such matters; and*
>
> *(ii) prepare assessments and reports in relation to such matters in accordance with the Government's requirements;*
>
> *(d) to:*
>
> *(i) assemble, correlate and analyse information relating to other matters that are of political, strategic or economic significance to Australia; and*
>
> *(ii) prepare assessments and reports in relation to such matters in accordance with the Government's requirements;*
>
> *if doing so would support the performance of any other function or the Director-General's functions, or complement the work of the national intelligence community;*

226. The Explanatory Memorandum indicates that the policy intent underlying these broader amendments is to ensure that:

- the requirements in the privacy rules governing the communication of personal information do not inadvertently apply to internal agency information relevant to matters of staffing and administration; and
- more broadly, to limit the application of the privacy rules regulating the communication of information to the actual intelligence produced by ONI (being information to which ONI had applied its analysis, to the exclusion of the 'raw information' it had obtained).[96]

Law Council views: additional amendments

227. The Law Council does not necessarily object to the enactment of those of the Schedule 10 measures which exceed the scope of recommendation 12 of the Richardson Review (noting that the latter recommendation was confined to information obtained via the performance of ONI's open source function).

228. However, the Law Council suggests that there is a need for further explanation of the reasons for including these additional measures. For the reasons outlined

[95] This is achieved through the definition of 'intelligence information' in proposed subsection 53(1C) and the limitation of proposed paragraph 53(1A)(b) to the communication of 'intelligence information that is personal information'.

[96] Explanatory Memorandum, 91 at [262].

below, there is also a need for further examination of their implications for the level of protection given to any confidential personal information that ONI obtains through means other than the performance of its open source function.

229. In particular, in making its recommendation 12, the Richardson Review appeared to be persuaded by a view that the privacy risks were lower in relation to the subsequent disclosure of personal information obtained by ONI in the performance of its open source function in paragraph 7(1)(g) of the ONI Act, because that information was necessarily already publicly available, and for this reason it was justifiable to remove such information from the scope of the privacy rules.[97]

230. However, if ONI obtains personal information from other sources for the purpose of performing its analytic functions in paragraph 7(1)(c) or 7(1)(d) of the ONI Act, that information will not necessarily be publicly available, and its subsequent disclosure by ONI may therefore be capable of raising significant privacy risks.

231. For example, it seems possible that assessments and reports prepared by ONI under paragraphs 7(1)(c) and (d) may utilise personal information about an Australian person, which has been collected by another Australian intelligence agency (such as ASIS or ASIO) or a foreign partner, and shared with ONI. That information may be sensitive and confidential in its own right, irrespective of whether it is subsequently integrated into an intelligence 'product', such as a report, comprising ONI's analysis and evaluation of that information.

232. Accordingly, the privacy risks associated with ONI communicating the 'raw personal information' it received, in the absence of it having applied independent analysis to that information, may nonetheless be significant. It is unclear why the privacy rules of ONI should not be required to govern the communication of such personal information, and why the statutory obligation imposed on ONI to comply with those rules in new paragraph 53(1A)(b) should not apply in these circumstances. As the extrinsic materials to the Bill do not clearly address this matter, the Law Council suggests that there would be value in the Committee pursuing it with the proponents of the Bill.

233. The justification provided in the Explanatory Memorandum appears to indicate that the exclusion of 'raw information' obtained in the course of performing the functions in paragraphs 7(1)(c) and (d) reflects a high-level policy position that there should be a rigid statutory distinction drawn between 'intelligence' (being information which is processed and has had some degree of analysis applied to it) and 'information' (being the raw input to which analysis is applied).[98]

234. The Explanatory Memorandum also comments that the measures are considered proportionate because 'unlike other NIC agencies, ONI does not have covert or intrusive powers to collect intelligence (such as the ability to obtain warrants or conduct compulsory questioning) and ONI's functions do not include directing a NIC agency to carry out operational activities'.[99]

---

[97] Richardson Review, *Unclassified Report, Vol 1,* 256 at [11.67] citing ONI's submission that 'ONI agreed that privacy rules should continue to apply to the OSC's [Open Source Centre's] finished, 'analytical reports but queried whether the rules should apply "to publicly available raw information *where the privacy risk associated with sharing this information is low given it is already in the public domain*",' (emphasis added). See also 256-257 at [11.69]: 'In cases where ONI shares, but does not apply analysis to, identifiable information produced by another entity, *such as a news article,* ONI's privacy rules should not apply' (emphasis added). The italicised text in the quoted passage refers expressly to a type of information that is publicly available (a news article). The unclassified report of the Richardson Review does not comment specifically on the management of privacy risks associated with ONI sharing personal information which has been provided to it by other agencies, where that information is not otherwise publicly accessible.

[98] Explanatory Memorandum, 90-91 at [260]-[261].

[99] Ibid, 43 at [218].

235. However, the Law Council notes that the primary consideration underlying the requirement for ONI to be subject to privacy rules (in preference to the application of the Privacy Act) is the management of privacy risks arising from the collection, handling, communication, retention and destruction of personal information concerning Australian persons. A technical categorisation of personal information as being 'intelligence' or merely 'raw information' does not have any apparent bearing upon the level of privacy risk that may arise from its subsequent communication, and therefore the need for such communication to be governed by privacy rules, with the agency's compliance being subject to independent oversight by the IGIS.

236. Further, while ONI may not have intrusive intelligence collection powers, or powers to direct other agencies to collect intelligence, it could conceivably be the recipient of information obtained by other agencies or foreign partners in the exercise of their intrusive powers, which were exercised for the purpose of those agencies performing their respective functions. The absence of a statutory power enabling ONI to directly collect, or direct others to collect, the relevant personal information appears to be a separate matter to the privacy risks that may arise from the subsequent communication by ONI of personal information in its possession.

Schedule 11: Inclusion of ASD in the assumed identities regime

Key proposed amendments

237. Schedule 11 proposes to amend Part IAC of the *Crimes Act 1914* (Cth) (**Crimes Act**) to include ASD in the assumed identities regime, meaning that ASD officers would be able to operate and use false identities for the purpose of the proper performance by ASD of its statutory functions under the ISA. Currently, ASIO, ASIS and ONI are the only intelligence agencies included in the regime.

238. The Bill only proposes to enable ASD staff members to operate and use assumed identities, not to acquire evidence of an assumed identity (such as identity documents including false birth certificates). The latter function would continue to be performed by ASIO or ASIS, on behalf of ASD.[100]

239. The proposed amendments in Schedule 11 would result in ASD being subject to the same statutory record-keeping, reporting and associated oversight requirements as those which presently apply to ASIO. ASIS and ONI.[101] ASD's activities in relation to assumed identities would also be subject to IGIS oversight, as is presently the case for the other intelligence agencies included in the regime.

Law Council views

240. The Law Council acknowledges that a reasonable case has been advanced in relation to the necessity and proportionality of including ASD in the assumed identities regime. There could legitimately be circumstances in which the activities of ASD officers, if capable of being attributed to them in that capacity, may make it possible to deduce that ASD has or is likely to have a particular cyber-intelligence or counter-intelligence capability, or is seeking to acquire one, or is likely to be undertaking a particular operational activity. For example, if it is possible to deduce that ASD officers are likely to be using, or are likely seeking to acquire, a particular form of computer-related infrastructure or other technology, there is the potential for such information to be highly prejudicial to Australia's national security. This information could be exploited by targets of intelligence operations to ascertain that they are under investigation and engage in counter-intelligence measures to evade

[100] Bill, Schedule 11, item 10 (inserting new paragraph 15KI(2A)(d) of the Crimes Act).

[101] Crimes Act, Subdivision B of Division 6. (See also the offences for misuse of assumed identities by agency staff in Subdivision A, which would similarly apply to ASD staff members.)

detection; or by hostile State or non-State actors to take offensive measures against Australia's cyber security.

241. The Law Council notes that, if ASD is presently managing these risks by utilising the assumed identities regime via its cooperation with ASIO or ASIS, as is permitted under these agencies' respective governing legislation,[102] then the interests of transparency would be more effectively served via ASD's direct inclusion in the assumed identities regime. That is, it would be more transparent for the Crimes Act to explicitly acknowledge and directly regulate the use of assumed identities by ASD, rather than effectively operating 'by proxy' via ASD's cooperation with ASIO or ASIS. The direct regulation of ASD under the regime may also simplify the applicable lines of approval and reporting, which could more effectively facilitate accountability and oversight.

Schedule 12: Meaning of 'authorities' of other countries in the ISA

Key proposed amendments

242. Schedule 12 proposes to clarify the meaning of the term 'authority of another country' for the purpose of the cooperation provisions in section 13 of the ISA. As noted above in relation to the discussion of Schedule 6, existing paragraph 13(1)(c) of the ISA permits the ISA agencies to cooperate with authorities of other countries, for the purpose of the ISA agency performing its functions, subject to certain statutory requirements being met (including prior approval by the Minister).

243. The term 'authority of another country' is presently undefined in the ISA. The Explanatory Memorandum identifies that ISA agencies have identified ambiguity in the meaning of this term, and in particular whether it is limited to authorities which are established by a law of the foreign country, or are under the control of the internationally recognised government of another country. This may create doubt as to whether the Minister is legally able to authorise cooperation with entities which are exercising effective governmental control of all or part of a foreign country, but which are not internationally recognised as the government of that country. In turn, this may create uncertainty about the legal basis for any subsequent cooperation with that authority, including subsequent uses to which any intelligence obtained from that cooperation may be put.[103]

244. The proposed amendments in Schedule 12 seek to address this ambiguity by inserting a non-exhaustive definition in section 3 of the ISA. The proposed definition provides that it does not matter whether the relevant body is established by a law of the other country, or is connected with an internationally recognised government of the country.

Law Council views: ISA amendments

245. The Law Council acknowledges that it is strongly preferable for the ISA to provide a high degree of definitional clarity and certainty, given the degree of intrusion of the activities authorised; the breadth of corresponding immunities conferred; and the covert nature of intelligence operations, which reduces the likelihood that its provisions will be the subject of judicial review and interpretation.

246. Moreover, the Law Council does not object to the explicit inclusion of non-statutory bodies and bodies which are not part of internationally recognised governments. In particular, this will ensure that there is a clear legal basis upon which agencies can undertake cooperation in circumstances of civil conflict or unrest in foreign countries in which the body in effective governmental control of an area is not

[102] This is explicitly acknowledged in the Explanatory Memorandum, 44 at [224] and 95 at [292], which also identifies that this practice is inefficient and 'proving unsustainable in the current operational environment'.
[103] Explanatory Memorandum, 47 at [242].

internationally recognised as its government. It will also make explicit that Ministerial approval is needed in relation to that cooperation, as a legal pre-condition to undertaking those activities.

247. The Law Council's previous comments on Schedule 6, in relation to potential human rights risks arising from ISA agencies' cooperation with foreign governments, apply with even more force to the cooperative activities of ASIS, ASD and AGO with respect to the sharing of intelligence or intelligence collection capabilities or support, and the tasking of foreign authorities to collect intelligence. The intelligence obtained may be more sensitive than other forms of information and may involve far more intrusive methods of collection.

248. Accordingly, the proposed amendments in Schedule 12 may offer a timely opportunity for the Committee to obtain further information from ISA agencies about their current decision-making and governance arrangements, in identifying and managing the risk that their cooperation with an authority of a foreign country could enable the relevant foreign government, whether internationally recognised or *de facto*, to engage in human rights violations against its own citizens or others.

Potential need for corresponding amendments to section 13 of the ONI Act

249. Further to the discussion in relation to Schedule 7 above, the framework for cooperation in section 13 of the ONI Act also adopts the term 'authority of another country'. This expression is similarly undefined in the ONI Act. Accordingly, there may be similar ambiguity as to whether the expression, as used in the ONI Act, covers cooperation with bodies which are exercising *de facto* governmental control of all or part of another country, but which are not internationally recognised as the governments of those countries.

250. This creates a risk that DG-NI approval may not be required for such cooperation should ONI identify a need for it, on the basis that such bodies are taken to be 'entities' rather than 'authorities of another country' (noting that only ONI's cooperation with 'authorities of another country' is subject to the prior DG-NI approval requirement and the Prime Ministerial 'veto' power in relation to DI-NI approvals under section 13 of the ONI Act).

251. The Law Council therefore queries whether there would be benefit in also amending section 13 ONI Act to include the same clarification as that proposed in Schedule 12 in relation to the ISA. The Committee may wish to consider exploring this matter with the proponents of the Bill and ONI.

Schedule 13: ASIO authorisations—'future positions' clarification

Key proposed amendments

252. Schedule 13 to the Bill proposes to amend provisions in section 24 of the ASIO Act and section 12 of the TIA Act, which confer powers on ASIO officials to authorise persons to exercise authority under ASIO's special powers and telecommunications interception warrants. It would implement recommendations 37 and 103 of the Richardson Review, which identified some ambiguities in the drafting of existing authorisation provisions.

253. Presently, these provisions empower the Director-General of Security, or another person appointed by the Director-General, to authorise persons to exercise authority under an ASIO warrant. Section 24 of the ASIO Act expressly permits the authorisation of classes of persons, but does not expressly extend to 'future positions'. That is, persons whose position or office falls within the class prescribed in the instrument of authorisation (for example, all persons holding a particular job title, at a particular classification, within a particular administrative unit in ASIO) but their particular position or office (for example, an individual intelligence officer

position within the specified administrative unit) was created after the authorisation was given. Moreover, section 12 of the TIA Act contains no explicit provision in relation to class authorisations.

254. The Richardson Review considered that this lack of clarity was undesirable in the context of provisions authorising individuals to exercise highly intrusive powers.[104] The amendments in Schedule 13 to the Bill seek to provide clarity on the face of the relevant authorisation provisions in the ASIO Act and TIA Act. While technical in nature, these measures are important because there is some doubt as to whether it is legally possible, at common law, for a power of authorisation in favour of a class of persons by reference to their positions or offices to include an individual whose position or office had not come into existence at the time the authorisation was given—even if as, a matter of fact, the individual position or office fell within the broad class of positions specified in the instrument. The *Acts Interpretation Act 1901* (Cth) (**Acts Interpretation Act**) was amended in 1994 to remove this risk in relation to powers of delegation alone, further to intermediate court decisions that powers of delegation exercised in favour of classes of persons could not extend to 'future positions'.[105] Section 34AA of the Acts Interpretation Act provides that powers of delegation are taken to cover 'future positions' and not merely the positions within a specified class that were in existence at the time the power was exercised. However, the matter appears to be unresolved in relation to authorisations, since the Acts Interpretation Act does not contain an equivalent general interpretive rule to that in section 34AA for delegations.

Law Council views

255. The Law Council supports the position taken in the Richardson Review, which endorsed agency submissions indicating that it would be prudent for individual provisions conferring powers of authorisation to specify that powers to authorise classes of persons cover 'future positions' falling within the class, wherever this is the policy position.[106]

256. Similar clarificatory provisions to those proposed in Schedule 13 exist in authorisation provisions contained in other Commonwealth Acts.[107] It is desirable that the legislation governing the authorisation of persons to exercise intrusive powers for and on behalf of ASIO takes a consistent approach with existing legislation conferring investigatory powers. This will provide a consistent degree of clarity and certainty for agencies, individuals exercising authority under warrants, and persons who are the subject of intrusive warrant-based powers.

257. The Law Council also has no concern with the policy position of expressly permitting, rather than prohibiting, the power of authorisation to be exercised in favour of 'future positions'. It is acknowledged that agency organisational structure and operational requirements can change rapidly, including in response to changes in the security environment. In the absence of the Acts Interpretation Act creating a general rule of statutory interpretation that powers of authorisation apply to 'future positions' (as it does in section 34AA for powers of delegation) it is desirable that the matter is managed by individual provisions conferring specific powers of authorisation. The alternative is that new instruments of authorisation

[104] See, for example, Richardson Review, *Unclassified Report, Vol* 2, and 94 at [19.82] and rec 37.

[105] See, for example, *Australian Chemical Refiners Pty Ltd v Bradwell* (unreported NSW Court of Criminal Appeal, 28 February 1986) in which it was held that a power of delegation to commence a prosecution, which was exercised in favour of a class of persons by reference to position, did not extend to an individual position which came into existence after the power of delegation was exercised, on the basis that the instrument of delegation was taken to be speaking at the time it was made. See further: *Law and Justice Legislation Amendment Act 1994* (Cth), section 5; and Explanatory Memorandum, Law and Justice Legislation Amendment Bill 1994, 5 at [8].

[106] Richardson Review, *Unclassified Report, Vol 2*, 93-94 at [19.17]-[19.81].

[107] See, for example, *Customs Act 1901* (Cth), subsection 4(1A).

would need to be made each time a new position is created which is covered by the class specified in an instrument of authorisation. This may be inefficient.

258. However, as a more general observation about the authorisation of persons to exercise the intrusive, warrant-based intelligence collection powers of ASIO, the Law Council notes the importance of instruments of authorisation adequately particularising the relevant class of persons; and that class being limited to people with appropriate skills and experience; as well as the agency having adequate arrangements for the supervision and control of the actions of those persons in executing warrants.

259. The independent operational oversight of the IGIS, including as part of the routine inspection of ASIO warrants, will continue to provide valuable assurance about these matters. Such assurance may become even more important if the explicit coverage of 'future positions' results in a 'net widening' of the classes of persons who are authorised to exercise powers under ASIO's intelligence collection warrants.

Schedule 14: Minor error correction measures in the ISA

Key proposed amendments

260. Schedule 14 to the Bill proposes to rectify some drafting errors in relation to the functions of ASD, which are outstanding from the enactment of legislation in 2018 to establish that agency on a statutory basis, in line with a recommendation of the IIR (noting that, previously, ASD was administratively part of the Department of Defence).[108] In particular, the measures in Schedule 14 propose to:

- correct inaccurate cross-references to provisions in section 13 (item 2); and
- address an unintended omission of a statutory maximum period of effect for MAs issued to ASD under subparagraph 8(1)(a)(iii) for the purpose of that agency undertaking activities outside Australia to disrupt cybercrime suspected of being committed or enabled by an Australian person (item 1). (The latter MA mechanism, and the underlying cybercrime prevention and disruption function of ASD in paragraph 7(1)(c), was also inserted by the 2018 amendments which established ASD as a statutory agency.)

Law Council views

261. The Law Council concurs with the assessment in the Explanatory Memorandum that these measures are fairly described as technical corrections of drafting errors or omissions, which will not impact significantly on the rights and liberties of individuals.[109] Accordingly, the Law Council has no substantive concerns with the measures in Schedule 14.

262. Importantly, the explicit imposition of a six-month maximum period of effect for ASD's cybercrime-related MAs would remove the legal power to issue authorisations that are in force in perpetuity, which would thereby provide a stronger safeguard.

263. As with other grounds of ministerial authorisation in section 8 of the ISA, if an ISA agency identifies a need to conduct an intelligence collection activity in relation to an Australian person for longer than six months, they will need to make a request to the Minister for a further authorisation, and complete all reporting requirements for the expired authorisation. This ensures that, even for prolonged operations,

[108] *Intelligence Services Amendment (Establishment of the Australian Signals Directorate) Act 2018* (Cth). See also, IIR, *Unclassified Report*, recommendation 6.

[109] Explanatory Memorandum, 49 at [254] and 103 at [344].

there are periodic checks on their necessity and proportionality (including giving consideration to applying specific conditions or limitations to the authorisation).

264. Given the description of the proposed amendment as correcting an unintended omission, it appears that this may be the present administrative practice adopted by ASD and the Defence Minister. However, an explicit statutory maximum period of effect of six months will remove any legal ability for a single authorisation to last longer if there was a desire for it to do so in future.