Law Council
OF AUSTRALIA

Comprehensive review of the legal framework governing the National Intelligence Community

Dennis Richards AO
Attorney-General's Department

28 November 2018

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

Table of Contents

About the Law Council of Australia

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

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

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

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

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

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

Members of the 2018 Executive as at 1 January 2018 are:

- Mr Morry Bailes, President
- Mr Arthur Moses SC, President-Elect
- Mr Konrad de Kerloy, Treasurer
- Mr Tass Liveris, Executive Member
- Ms Pauline Wright, Executive Member
- Mr Geoff Bowyer, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council acknowledges the assistance of its National Criminal Law Committee in the preparation of this submission.

Executive Summary

1. The Law Council welcomes the opportunity to provide a submission to the Attorney-General's Department (**Department**) regarding the Comprehensive review of the legal framework governing the National Intelligence Community (**Review**), led by Dennis Richardson AO.

2. The Law Council understands the Review follows a recommendation made by Professor Michael L'Estrange AO and Mr Stephen Merchant PSM who undertook the 2017 Independent Intelligence Review (**IIR**). The IIR recommended there be a comprehensive review of the Acts governing Australia's intelligence community to ensure agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians. The IIR recommended this comprehensive review consider the different warrant thresholds across various Acts which may create uncertainty.

3. The Law Council previously wrote to the Prime Minister, the Attorney-General, the Minister for Foreign Affairs, the Minister for Defence, the Minister for Home Affairs, the Independent National Security Legislation Monitor (**INSLM**) and the Inspector-General of Security and Intelligence (**IGIS**) offering its views and assistance following the IIR. The Law Council directs the Review to the views expressed in that letter, which is attached to this submission.

4. The Law Council notes that the Terms of Reference for the Review do not specifically include consideration of whether the legislative framework for the National Intelligence Community (**NIC**) is consistent with the rule of law and that it is both necessary and proportionate. The Law Council considers that this is a critical limitation of the Review. However, as Mr Richardson has requested the Law Council to provide a view on the philosophy and principles underpinning the existing legislation governing the NIC, this submission makes several recommendations in this regard.

5. The Law Council considers that legislation governing the NIC requires a careful and deliberate response. NIC agencies must be well-equipped to face national security threats. The Australian Government has a primary responsibility to protect the life and security of the person. However, in order to preserve the values that underpin our democratic society, Australia's laws must be reasonable, necessary and proportionate to achieve a legitimate objective.[1]

6. The Law Council regularly provides submissions in relation to federal Parliamentary inquiries which examine and invest the NIC with extensive and intrusive powers to perform their functions. The Law Council has raised concerns that many of these powers:

    - have not been shown to be a necessary or proportionate response to the threats to national security facing Australia;
    - are excessive in their breadth and reach;
    - impinge upon Australia's international human rights obligations; and
    - lack inbuilt mechanisms for accountability.

[1] This also accords with international human rights law – see Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Human Rights Scrutiny Report* (2015) 6.

7. Key recommendations made in this submission include:

- A further principle underpinning the NIC should include consistency of its legislative framework with the rule of law. The Law Council's *Policy Statement: Rule of Law Principles* may be instructive in this regard.[2]
- A charter or bill of rights should be developed so that any common legislative framework governing the NIC must be compatible with Australia's international human rights obligations.
- A single, consistent privacy impact test should be implemented to ensure that privacy considerations are always taken into account before a warrant to intercept or access a telecommunication is granted or access to telecommunications data is authorised.
- Where there is information collected about foreign actors, collection of information about that threat should meet thresholds that are appropriate to that threat, the relevant collection activity and international obligations.
- Regarding amendments to the Ministerial Authorisation (**MA**) regime, the Law Council recommends:
  - confining the proposed MA power to persons involved with listed terrorist organisations under the *Criminal Code Act 1995* (Cth) (**Criminal Code**).
  - requiring the agreement of the Attorney-General as the First Law Officer with oversight by the IGIS (as a minimum).
  - specifying the maximum duration of the class authorisation, although the Law Council encourages the Australian Government to consult with the IGIS and INSLM as to whether a 6 month period is appropriate.
  - keeping of a current list of the Australians on whom they are seeking to produce intelligence under the authorisation, outlining the justification for their continued coverage.
- The second INSLM's recommendation be implemented that a protocol should be developed between the Australian Security Intelligence Organisation (**ASIO**), the Australian Criminal Intelligence Commission (**ACIC**), and any relevant state body which shares information obtained by compulsory questioning, to avoid oppression by successive examinations. This protocol should then be approved and given appropriate status by the Attorney–General. The INSLM and other supervisory bodies such as the IGIS and the Commonwealth Ombudsman should be able to monitor how this protocol operates in practice.[3]
- The IGIS or Commonwealth Ombudsman should be empowered to make a proportionality determination where multiple powers are employed against an individual.
- The Review should consider legislative amendments that provide greater distinction between the types of conditions that may trigger each agency exercising their particular powers.
- The Review should consider how agency employees and the community can be better educated regarding the conditions that may trigger each agency exercising their particular powers.

[2] Law Council of Australia, Policy Statement on Rule of Law Principles (March 2011).
[3] Independent National Security Legislation Monitor The Hon Roger Gyles AO QC, *Certain questioning and detention powers in relation to terrorism* (October 2016), 2.

- Any sharing of information between NIC agencies, and between NIC agencies and Commonwealth, State, Territory, foreign government or other partners, should be done in a manner consistent with the privacy principles contained in the *Privacy Act 1988* (Cth).
- If the co-operation regime for activities undertaken in relation to ASIO is extended to all *Intelligence Services Act 2001* (Cth) (**ISA**) agencies and to activities undertaken both within and outside Australia, some of the circumstances in which it is anticipated that cooperation between ASIO and other ISA agencies not currently captured are required should be clearly articulated.
- The Review should consider recommending a comprehending revision of the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**), with for example urgent amendments to:
  - introduce defined limits on the issue of B-party warrants and the derivative use of material collected by a B-party warrant;
  - increase the penalty thresholds for stored communications warrants to apply only to criminal offences; and
  - increase the threshold for sharing stored communications to that prescribed in sections 110 and 139 of the TIA Act.[4]
- A comprehensive review of the TIA Act should also consider the need for judicial warrant for access to telecommunications data.
- The Review consider legislative amendments that introduce a greater level of oversight and accountability into the existing regime for authorising access to and disclosure of telecommunication data by certain enforcement and intelligence agencies. This may include replacing a system of authorisations for accessing and disclosing prospective telecommunications data with a warrant-based system.[5]
- The outstanding recommendations of the Australian Law Reform Commission's (**ALRC**) Report *Secrecy Laws and Open Government in Australia* (**the Secrecy Report**) should be implemented, including:
  - The general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to:
    - damage the security, defence or international relations of the Commonwealth;
    - prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;
    - endanger the life or physical safety of any person; or
    - prejudice the protection of public safety.
  - In the absence of an express harm requirement secrecy offences should cascade in penalty and require that a person knew, or as a lesser offence, was reckless as to whether, the protected information falls within a particular category (i.e. security classification or concerns

[4] See the Law Council of Australia Submission to the Senate Standing Committee on Legal and Constitutional Affairs *Comprehensive Review of the Telecommunications (Interception and Access) Act 1979,* 14 March 2014.
[5] Law Council of Australia, Submission to the Senate Legal and Constitutional Affairs Committee, *Telecommunications Amendment (Get a Warrant) Bill 2013,* 31 July 2018.

Australia's national security), and should not provide that strict liability applies to that circumstance.

- There should be a public interest defence, rather than a 'journalist' defence which includes the term 'news media', the meaning of which is uncertain.

- Adequate exemptions should always be provided to preserve client legal privilege and the confidentiality between a lawyer and their client.
- Recommendation 16(c) of the IIR be implemented: Introducing a requirement for all ISA agencies to seek a Ministerial Authorisation for activities likely to have a direct effect on an Australian person.
- The examination of an accused person by ASIO and the ACIC should be deferred until after the disposition of any charges.
- In the alternative, the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**) and *Australian Crime Commission Act 2002* (Cth) (**ACC Act**) should require authorisation from a Federal Court judge before a summons is issued to a person who is subject to criminal proceedings, and for that Judge to prescribe limitations on the matters which may be covered by the examination.
- In relation to the *National Security Information (Criminal and Civil Proceedings) Act 2004* (**NSI Act**)*,* the Review consider making the following recommendations:
  - defendants and their legal representatives could only be excluded from hearings in limited specified circumstances, and that courts would retain the power to stay proceedings if the defendant could not be assured of a fair trial;[6]
  - when making an order allowing information to be disclosed subject to the Attorney-General's non-disclosure certificate, the court should be satisfied that any amended document and/or substitution documentation to be adduced as evidence would provide the defendant with substantially the same ability to make his or her defence as would disclosure of the source document;[7]
  - when making an order to exclude a witness from the proceedings, the court should be satisfied that the exclusion of the witness would not impair the ability of the defendant to make his or her defence;[8]
  - sections 39 and 39A of the NSI in relation to the security clearance process be repealed;
  - In the alternative, the Law Council recommends that sections 39 and 39A be amended so as to give the court a greater role in both determining whether a notice should be issued and in reviewing a decision to refuse a legal representative a security clearance.[9]

[6] Senate Committee on Legal and Constitutional Affairs Report on the Provisions of the *National Security Information (Criminal Proceedings) Bill 2004 and the National Security Information (Criminal Proceedings) (Consequential amendments) Bill 2004,*19 August 2004, Recommendation 1.
[7] Ibid Recommendation 7.
[8] Ibid Recommendation 8.
[9] Ibid Recommendation 10.

- The outstanding recommendations of the INSLM in his third annual report should be addressed, for the reasons outlined in the INSLM's report.
- The Criminal Code and the ISA be amended to exclude economic relations from the definition of national security, and Australia's national economic wellbeing from the purpose of an intelligence agency's functions.
- The *Independent National Security Legislation Monitor Act 2010* (Cth) (**INSLM Act**) be amended so that:
  - there should be an express power for the INSLM to report on a matter or matters within the statutory mandate but more urgently or particularly than by the annual report. If this is accepted;
  - there be no possibility of reappointment of the INSLM; and
  - the Government be required to provide a public response to the INSLM's recommendations within six months.
- The IGIS, Ombudsman and INSLM offices should be allocated additional resources to fulfil any expanded responsibility.

Philosophy and principles underpinning the NIC

8. The philosophy and principles underlying the legislative framework and operations of the NIC remain based on the basic judgements from the first Royal Commission on Intelligence and Security by the Hon Justice Robert Hope, which reported in 1977.

9. In his tabling speech the then Prime Minister, the Hon Malcolm Fraser identified seven basic principles as arising from the Hope Royal Commission 1977 Report:

   (a) Australia needs a highly professional system of intelligence and security services;

   (b) Australia has faced, faces or may face threats to its internal security;

   (c) A balance must be achieved between the rights of individual persons and the preservation of the security of Australia as a nation;

   (d) Australia has a duty to protect classified information;

   (e) It would jeopardise national security to reveal the activities, programs and priorities of Australia's intelligence and security agencies;

   (f) Intelligence and security agencies should always comply with the law; and

   (g) Intelligence and security agencies should be subject to parliamentary oversight.[10]

10. The Law Council considers that it is vital that a further principle underpinning the NIC include consistency of its legislative framework with the rule of law. The Law Council's *Policy Statement: Rule of Law Principles* may be instructive in this regard.[11]

[10] Commonwealth, *Parliamentary Debates*, House of Representatives, 25 October 1977, 2334 (The Hon Malcolm Fraser).
[11] Law Council of Australia, Policy Statement on Rule of Law Principles (March 2011).

11. In addition, the Royal Commissioner outlined a number of principles specifically for ASIO as the domestic security agency, which also, however, reflect the broader philosophy underlying the legislative framework of the intelligence community:

    (a) That it [ASIO] operates within the terms of its statute and is concerned only with matter relevant to security.

    (b) That it always complies with the law.

    (c) And that it observes standards of propriety by not intruding on the rights and freedoms of persons except to the extent that the requirements of the nation's security justify, and the law allows.[12]

12. The balance between the needs for security and individual liberty are central throughout the Hope Royal Commission report and the systems implemented since then. The Law Council submits that this balance is critical to the rule of law which demands everyone is subject to the law and is entitled to its benefits.

13. Laws relating to the intelligence community must ensure that they provide for the freedom of Australian citizens and residents while maintaining their security and protecting Australian democracy. Effective and adequately resourced oversight and accountability arrangements are critical to ensure that agencies continue to comply with the law and observe standards of propriety and proportionality.

Recommendation

- **A further principle underpinning the NIC should include consistency of its legislative framework with the rule of law. The Law Council's *Policy Statement: Rule of Law Principles* may be instructive in this regard.[13]**

Adoption of a common legislative framework

14. The Review intends to address 'whether Australia should adopt a common legislative framework, as has been done in the United Kingdom and New Zealand'.

15. The Law Council notes that New Zealand and the United Kingdom have enacted legislation to move towards a single point of co-ordination for the intelligence community.[14] In New Zealand, the *Intelligence and Security Act 2017* replaced the four acts that previously applied to the two intelligence and security agencies and their oversight bodies. In the United Kingdom, the budgets of the three largest intelligence agencies are managed by a Single Intelligence Account, which has led to improvement of shared capabilities of the three agencies. The *Investigatory Powers Act 2016* has further contributed to a common legal regime for the three major intelligence agencies.[15]

16. The Law Council is of the view that common legislative frameworks are desirable to the extent of ensuring consistency. However, consistency should not be achieved at the

[12] Justice Robert Hope, *Royal Commission into on Intelligence and Security*, 'Fourth Report', paragraph 786, 1977.
[13] Law Council of Australia, Policy Statement on Rule of Law Principles (March 2011).
[14] Michael L'Estrange AO and Stephen Merchant PSM *Report of the 2017 Independent Intelligence Review* (18 July 2017), 55 [4.8].
[15] Ibid 54 [4.6].

expense of reduced safeguards, and there must be appropriate legislative recognition of the different functions that different NIC agencies perform.

17. The Law Council notes that legislative framework in the UK for its national security agencies is subject to the requirements of the *Human Rights Act 1998*, which incorporated the principles of the European Convention on Human Rights (**ECHR**) into UK law.[16] The application of the *Human Rights Act 1998* means that it is unlawful for intelligences agencies, as public authorities, to act in a way that is incompatible with the rights set out in the Act and the ECHR.

18. The Law Council has previously expressed its policy position in support of the development of a charter or bill of rights at the federal level.[17] The existing legal framework at the federal level fails to guarantee adequate protection for fundamental human rights. Insufficient prominence is afforded to human right within the existing framework, either as a set of principles to which the arms of government must have regard or as a set of principles by which the arms of government, including the national security agencies, are bound.[18] In the context of Australia's national security framework, certain rights are more likely to be engaged than others, such as the right to privacy,[19] the right to freedom of opinion and expression,[20] and the right to be free from arbitrary detention.[21] A charter or bill of rights should allow a person to have the right to bring proceedings against a public authority for violation of his or her human rights and to seek appropriate relief, excluding damages. It would also require the executive arm of government to comply with the human rights contained therein with a view of promoting a culture of respect for human rights within government.

19. In addition, as advances in technology and surveillance capabilities increase, the rights held by people offline must also be protected online, and all States must respect and protect the right to privacy in digital communication.[22] A General Assembly resolution further called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data. It emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law. The Law Council encourages the Review to turn its mind to the relevant international law principles, in particular the right to privacy as protected by Article 17 of the International Covenant on Civil and Political Rights,[23] when undertaking this review of the TIA Act.

20. As the Law Council has previously submitted, in order to protect against unjustified intrusion into personal privacy, surveillance legislation such as the TIA Act should contain a single, consistent privacy impact test to ensure that privacy considerations are

---

[16] UK Government, *National Intelligence Machinery Booklet* (19 November 2010), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61808/nim-november2010.pdf 3

[17] Law Council of Australia, *Policy Statement: a charter protecting the rights of all Australians* (29 November 2008).

[18] Ibid 2.

[19] *International Covenant on Civil and Political Rights*, opened for signature, 999 UNTS 171 (entered into force 23 March 1976), art 17 stating that (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; and (2) Everyone has the right to the protection of the law against such interference or attacks.

[20] Ibid art 19.

[21] Ibid art 9.

[22] The United Nations General Assembly resolution that the United Nations High Commissioner for Human Rights refers to is Resolution A/RES/68/167: The right to privacy in the digital age, 18 December 2013, at http://www.un.org/depts/dhl/resguide/r68_en.shtml.

[23] *International Covenant on Civil and Political Rights*, opened for signature, 999 UNTS 171 (entered into force 23 March 1976), art 17.

always taken into account before a warrant to intercept or access a telecommunication is granted or access to telecommunications data is authorised.

21. In its previous submissions, the Law Council has noted that privacy considerations are currently taken into account in the issuing of certain TIA Act warrants, but not all. The Law Council has recommended that a consistent privacy test be applied in all warrant applications and in all authorisations to intercept, access or disclose telecommunications data.

45. The key features of the test proposed by the Law Council can be summarised as follows:

    Before authorising the use of an interception, access or disclosure power under the TIA Act the authorising officer must:

    - *consider whether the exercise of the interception, access or disclosure power would be likely to deliver a benefit to the investigation or inquiry; and*
    - *consider the extent to which the interception, access or disclosure is likely to interfere with the privacy of any person or persons; and*
    - *be satisfied on reasonable grounds that the benefit likely to be delivered to the investigation or inquiry substantially outweighs the extent to which the interception, access or disclosure is likely to interfere with the privacy of any person or persons.*

Recommendations

- **A charter or bill of rights should be developed so that any common legislative framework governing the NIC must be compatible with Australia's international human rights obligations.**
- **A single, consistent privacy impact test should be implemented to ensure that privacy considerations are always taken into account before a warrant to intercept or access a telecommunication is granted or access to telecommunications data is authorised.**

Distinction between foreign intelligence and security intelligence

22. The Law Council notes that, as a Term of Reference, the Review intends to address 'the appropriateness of maintaining the current distinction between Foreign Intelligence and Security Intelligence, and legislative distinctions and restrictions relating to intelligence collection onshore and offshore'.

23. The Law Council considers that the distinction between foreign and security intelligence should be maintained.

24. The Australian Government has a responsibility to protect the safety and security of Australians (including Australian citizens and residents) and to protect the democratic values underpinning the Australian Constitution. To do this the government needs to be able to address internal and external threats to our democracy and the rule of law.

25. Under the ASIO Act security refers to the *protection of* Australia (including the States) and Australians from espionage, sabotage, politically motivated violence, the promotion

of communal violence, attacks on Australia's defence system or acts of foreign interference (section 4).

26. Under the ASIO Act foreign intelligence means *intelligence about* the capabilities, intentions or activities of people or organisations outside of Australia (section 4). Foreign intelligence is collected by ASIS, ASD and AGO in a foreign country, or by ASIO in Australia.

27. Fundamentally the difference relates to security intelligence being about the protection of certain basic freedoms in Australia, whereas foreign intelligence is about the collection of information about potential threats posed by foreign actors.

28. As such, security and foreign intelligence agencies have to meet different requirements in order to exercise their powers. While an Australian may pose a security threat, in order for a security investigation to occur certain thresholds have to be met. Furthermore, security intelligence may also inform administrative or law enforcement action, and again, therefore, require a high threshold for such an activity to occur. If the Australian Government is to take actions against an Australian, whether investigative, administrative or law enforcement, such an action should meet the highest standards of propriety.

29. Different thresholds are appropriate to a foreign actor outside of Australia. Foreign intelligence collection does not lead to administrative or law enforcement activity against Australians under Australian law. The thresholds to undertake foreign intelligence collection activity against foreign actors may therefore be different to those of security intelligence, but should still be subject to oversight and accountability. As the Australian Government is here not taking administrative or law enforcement action against an Australian (citizen or resident) but is merely collecting information about a foreign actor, collection of information about that threat should meet thresholds that are appropriate to that threat, the relevant collection activity and international law obligations.

30. The Royal Commission into Australian intelligence and security agencies conducted by Mr Justice Hope in 1974-1977 and 1983-84 (**Hope Royal Commission**) saw a vital distinction between foreign and security intelligence, as the traditional distinction underpinned an emphasis on the special rights to privacy and civil liberties of Australian persons, and it was appropriate to keep the work of ASIO and ASIS as two separate organisations. The IIR agreed with this distinction, stating that the separation 'continues to be important and the privileging of Australian persons in the mandates of particular Australian intelligence agencies and in Australian law remains strong',[24] despite economic globalisation, applications of new technologies, and the rising influence of non-state actors. Further, 'foreign and security intelligence continue to retain important distinguishing characteristics in terms of their operation context as well as Ministerial and legal accountability'.

Recommendation

- **Where there is information collected about foreign actors, collection of information about that threat should meet thresholds that are appropriate to that threat, the relevant collection activity and international obligations.**

[24] Michael L'Estrange AO and Stephen Merchant PSM *Report of the 2017 Independent Intelligence Review* (18 July 2017), 36, [2.22]

Ministerial authorisations

31. Australia's foreign intelligence agencies may in certain circumstances collect intelligence on Australians if they can obtain a Ministerial Authorisation (**MA**) from their responsible Minister.

32. The Law Council notes the recommendation of the IIR regarding amendments to the ministerial authorisation regime in the ISA:

> *Recommendation 16: Amendments to the Ministerial authorisation (MA) regime in the Intelligence Services Act 2001 (ISA) and associated processes be made to address practical difficulties arising from implementation of the regime. Such amendments, to be pursued in advance of the comprehensive review recommended above, would include:*
>
> *a) Introducing a class-based MA regime to enable ISA agencies to produce intelligence on a class of Australian persons involved with proscribed terrorist organisations. The class authorisation should be issued by the responsible Minister with the agreement of the Attorney-General and overseen by the Inspector-General of Intelligence and Security (**IGIS**). Class authorisations should last for a maximum period of six months but could be renewed. ISA agencies should maintain a current list of the Australians on whom they are seeking to produce intelligence on under the authorisation, outlining the justification for their continued coverage. Agencies should have to report to the responsible Minister within six months of the original authorisation.*

33. The Law Council recognises the importance of expeditious and judicious intelligence gathering on Australians involved with international terrorist groups which pose an actual or potential threat to other Australians.

34. However, class-based MA regimes enabling ISA agencies to produce intelligence on a class of Australian persons must be narrowly confined to ensure that broad categories of innocent Australians are not inadvertently captured.

35. If Recommendation 16(a) of the Review is implemented, the Law Council supports:

    (a) confining the proposed MA power to persons involved with listed terrorist organisations under the Criminal Code Indeed, in the context of the Counter-Terrorism Legislation Amendment Bill (No. 1) 2014 the Law Council recommended that the Bill be amended to include the types of permissible classes of Australian persons to which a class MA may apply and noted that restrictions to members of a listed terrorist organisation under the Criminal Code may be appropriate.[25]
    (b) requiring the agreement of the Attorney-General as the First Law Officer with oversight by the IGIS (as a minimum). As First Law Officer, the Attorney-General is well-placed to make assessments about the lawfulness of conduct by the AIC and to ensure that the AIC operates within the appropriate confines of the rule of law.
    (c) specifying the maximum duration of the class authorisation, although the Law Council encourages the Australian Government to consult with the IGIS and INSLM as to whether a 6 month period is appropriate. While renewals may be needed there should be a requirement for the agencies to establish the basis of

[25] Law Council of Australia, Submission No 16 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Counter-Terrorism Legislation Amendment Bill (No.1) 2014*, 11 November 2014, 21.

that need afresh each time an application is sought. This is paramount to ensuring that the exercise of the power is legitimately required.

(d) keeping of a current list of the Australians on whom they are seeking to produce intelligence under the authorisation, outlining the justification for their continued coverage. Agencies should be required to report to the responsible Minister within six months of the original authorisation. However, both of these safeguards should be required by legislation rather than left to administrative arrangements, which may be open to amendment by the agencies themselves without due oversight.

36. The number of Australian persons that the Australian Secret Intelligence Service (**ASIS**) produces intelligence on is likely to increase, should this recommendation of the Review be implemented.

37. Primary legislation should therefore clarify what types of activities could be approved for the purpose of:

(a) producing intelligence on one or more members of a class of Australian persons; or

(b) producing intelligence that will, or is likely to, have a direct effect on one or more members of a class of Australian persons.

38. While the legislation would not need to provide an exhaustive list of examples of what activities could be approved, further legislative guidance for the public would be beneficial.

39. IGIS oversight of the production of intelligence on Australian persons by ASIS is also likely to increase, as is the potential for ASIS to communicate intelligence on a class of Australian persons to other organisations (foreign and domestic). The office of the IGIS's annual budget should be supplemented to the extent required to provide for the new oversight requirements associated with implementation of the Review's recommendations (also discussed below).

Recommendations

- **Regarding amendments to the Ministerial Authorisation regime, the Law Council recommends:**
  - **confining the proposed MA power to persons involved with listed terrorist organisations under the Criminal Code.**
  - **requiring the agreement of the Attorney-General as the First Law Officer with oversight by the IGIS (as a minimum).**
  - **specifying the maximum duration of the class authorisation, although the Law Council encourages the Australian Government to consult with the IGIS and INSLM as to whether a 6 month period is appropriate.**
  - **keeping of a current list of the Australians on whom they are seeking to produce intelligence under the authorisation, outlining the justification for their continued coverage.**

Improvements to the legislative framework of the NIC

Co-ordination of NIC agencies' exercise of intelligence powers and functions

40. The Review intends to address 'improvements to the facilitation of the general co-ordination and appropriate control and direction of each agency comprising the NIC in relation to the exercise of intelligence powers and functions, and of the NIC as a whole.'

41. The Law Council notes the importance of ensuring consultation between Australia's national security agencies, in order to avoid excessive use of multiple powers on individual cases. The Law Council has previously called for clarification in this area[26] and it supports the finding of the second INSLM that:

> *A protocol should be developed between the Australian Security Intelligence Organisation, the Australian Criminal Intelligence Commission, and any relevant state body which shares information obtained by compulsory questioning, to avoid oppression by successive examinations. This protocol should then be approved and given appropriate status by the Attorney–General. The Independent National Security Legislation Monitor and other supervisory bodies such as the Inspector–General of Intelligence and Security and the Commonwealth Ombudsman should be able to monitor how this protocol operates in practice.*[27]

42. Confining certain powers to a single agency may arguably be inefficient and not allow the multiple aspects of terrorism to be addressed and investigated. A degree of overlap may also be beneficial for appropriate and lawful intelligence sharing, which is integral to addressing national security risks. There is a balance to be struck between sufficient separation to enable specialist agencies to perform their unique roles and ensuring that information is obtained in a consistent manner with rule of law principles and human rights obligations.

43. Nonetheless, there may be consequences to the overlap which should be considered and addressed. Any proposed law reform should be considered in the context of the whole range of existing laws.

44. Some consequences of the overlap which may impact on the necessity and proportionality of the powers include the potential:

- to create uncertainty about legal rights and obligations;
- for unnecessary duplication; and
- that the powers may be used in close succession exacerbating concerns regarding limitations on individual rights.

45. Accordingly, there would be merit in having the greatest possible clarity in distinguishing between the boundaries between the agencies to avoid unnecessary duplication and possible concurrent operation, and provide greater certainty to the operation of the different regimes.

---

[26] Law Council of Australia, Submission No 4 to the Parliamentary Joint Committee on Security and Intelligence, *Review of ASIO's questioning and detention powers*, 19 April 2017; Law Council of Australia, Submission to the Independent National Security Legislation Monitor, *Questioning and detention powers,* 16 June 2016,

[27] Independent National Security Legislation Monitor The Hon Roger Gyles AO QC, *Certain questioning and detention powers in relation to terrorism* (October 2016), 2.

46. The Law Council recognises that the Commonwealth Ombudsman or the IGIS may oversee the appropriateness of particular investigations. It also recognises the important role of the INSLM in reviewing the effectiveness of national security laws. However, it is concerned that there does not appear to be independent oversight of the proportionality of a range of measures in relation to a person *before* those measures are exercised.

47. The IGIS or Commonwealth Ombudsman should be empowered to make a proportionality determination where multiple powers are employed against an individual.

48. Legislative amendment should also be considered to provide greater distinction between the types of conditions that may trigger each agency exercising their particular powers. Education of agency employees and the community to raise awareness in this area should also be considered.

Recommendations

- **The second INSLM's recommendation be implemented that a protocol should be developed between ASIO, ACIC, and any relevant state body which shares information obtained by compulsory questioning, to avoid oppression by successive examinations. This protocol should then be approved and given appropriate status by the Attorney–General. The Independent National Security Legislation Monitor and other supervisory bodies such as the Inspector–General of Intelligence and Security and the Commonwealth Ombudsman should be able to monitor how this protocol operates in practice.**[28]
- **The IGIS or Commonwealth Ombudsman should be empowered to make a proportionality determination where multiple powers are employed against an individual.**
- **The Review should consider legislative amendments that provide greater distinction between the types of conditions that may trigger each agency exercising their particular powers.**
- **The Review should consider how agency employees and the community can be better educated regarding the conditions that may trigger each agency exercising their particular powers.**

Co-operation between NIC agencies and government

49. The Review intends to address improvements that could be made to ensure that the legislative framework for the NIC that 'support effective co-operation, liaison and sharing of information between NIC agencies, and between NIC agencies and Commonwealth, State, Territory, foreign government and other partners, for intelligence purposes'.

50. The Law Council is of the view that any sharing of information between NIC agencies, and between NIC agencies and Commonwealth, State, Territory, foreign government or other partners, should be done in a manner consistent with the privacy principles contained in the *Privacy Act 1988* (Cth).

51. The privacy principles of most concern when considering the functions of NIC agencies include:

[28] Ibid.

- Open and transparent management of personal information, by ensuring that they will comply with the Australian Privacy Principles (**APPs**) that includes taking steps to implement practices, procedures and systems that will enable, among other things, to deal with inquiries or complaints from individuals about the NIC agency's compliance with the APPs.
- Anonymity and pseudonymity – individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.
- Collection of solicited personal information – the entity must not collect personal information unless the information is reasonably the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.
- Notification of the collection of personal information – at or before the time or, if that is not practicable, as soon as practicable after, an entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances to notify the individual of such matters (for example, the purposes for which the APP entity collects the personal information).
- Security of personal information – if an entity holds personal information the entity must take such steps as are reasonable in the circumstances to protect the information from misuses, interferences, loss, unauthorised access, modification or disclosure.[29]

52. While intelligence agencies such as ASIO are not subject to the Privacy Act, they are nonetheless required to observe privacy considerations in the Guidelines. Observing fundamental privacy principles for the sharing of information between agencies is critical, particularly given the increasing potential to share sensitive personal information such as biometrics.

Recommendations

- **Any sharing of information between NIC agencies, and between NIC agencies and Commonwealth, State, Territory, foreign government or other partners, should be done in a manner consistent with the privacy principles contained in the *Privacy Act 1988* (Cth).**

Streamlined cooperation provisions

53. In relation to effective cooperation between NIC agencies, the Law Council refers to recommendation 18 of the IIR:

> *Recommendation 18: The co-operation provisions in Divisions 2 and 3 of Part 3 of the Intelligence Services Act 2001 (ISA) be streamlined to enhance co-operation amongst agencies. These changes, also to be pursued in advance of the comprehensive review recommended above, would include:*
>
> *a) clarifying that two ISA agencies co-operating with one another can act jointly under a single Ministerial authorisation from the relevant Ministers;*

[29] Office of the Australian Information Commissioner, *Privacy fact sheet 17*: *Australian Privacy Principles* (January 2014); available online https://www.oaic.gov.au/resources/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.pdf.

54. The Law Council would not oppose Recommendation 18(a) of the Review, subject to each ISA agency demonstrating their particular need for the authorisation and each of the relevant Ministers continuing to provide the relevant approval upon satisfaction of appropriate criteria.

> *b) extending the co-operation regime for activities undertaken in relation to the Australian Security Intelligence Organisation to all ISA agencies and to activities undertaken both within and outside Australia.*

55. The Law Council understands that implementation of Recommendation 18(b) may assist administration and avoid duplication.

56. Currently, not all ISA agencies can do less intrusive work in co-operation with ASIO (namely, those acts for which ASIO would not require a warrant in Australia). This appears to be because it is not within their functions to collect intelligence on Australians.

57. The changed threat environment whereby Australians may be involved as either perpetrators or victims of terrorism, espionage or foreign interference may require the cooperation regime to be broadened.

58. However, the need for implementation of this requirement should be clearly demonstrated, to ensure that public confidence in the AIC is maintained. This may be done for example by more clearly articulating some of the circumstances in which it is anticipated that cooperation between ASIO and other ISA agencies not currently captured are required.

59. The Law Council notes that it is important to ensure that the IGIS is appropriately resourced to maintain oversight over the arrangements where ISA agencies act on ASIO's behalf.

60. The Review's also intended to examine improvements that could be made to ensure that the legislative framework for the NIC support the intelligence purposes, functions, administration and staffing (including recruiting) of each agency comprising the NIC, and provide for accountability and oversight that is transparent and as consistent across the NIC agencies as is practicably feasible. The Law Council would support any additional support any additional resourcing, accountability and oversight of the NIC, as discussed below in relation to the IGIS and INSLM.

Recommendation

- **If the co-operation regime for activities undertaken in relation to ASIO is extended to all ISA agencies and to activities undertaken both within and outside Australia, some of the circumstances in which it is anticipated that cooperation between ASIO and other ISA agencies not currently captured are required should be clearly articulated.**

Specific proposals for reform

61. In light of the philosophical principles outlined above, the Law Council considers that there is a critical need for legislative reform in several areas of legislation underpinning the NIC. The listed areas are indicative only and should not be considered exhaustive. In the timeframe for the Review, the Law Council has focused on the below specific areas.

Telecommunications interception and access and surveillance legislation

62. Reform is required to ensure that the legislation is up-to-date and technology neutral while ensuring that robust safeguards are in place to protect an individual's rights and freedoms, client legal privilege and the confidentiality between a lawyer and their client.

63. The Law Council is of the view that there is a need for a comprehensive revision of the TIA Act with for example urgent amendments to:

- introduce defined limits on the issue of B-party warrants and the derivative use of material collected by a B-party warrant;
- increase the penalty thresholds for stored communications warrants to apply only to criminal offences; and
- increase the threshold for sharing stored communications to that prescribed in sections 110 and 139 of the TIA Act.[30]

64. The Law Council would support legislation that aims to introduce a greater level of oversight and accountability into the existing regime for authorising access to and disclosure of telecommunication data by certain enforcement and intelligence agencies, including any recommendations to replace a system of authorisations for accessing and disclosing prospective telecommunications data with a warrant-based system.[31]

65. The need for a judicial warrant for access to telecommunications data is particularly important when considering the breaches of section 7 of the TIA Act that may occur, which prohibits the interception of communications passing over a telecommunications system. ASIO self-reported three breaches of section 7 in the period 2017-2018.[32]

[30] See the Law Council of Australia Submission to the Senate Standing Committee on Legal and Constitutional Affairs *Comprehensive Review of the Telecommunications (Interception and Access) Act 1979* (14 March 2014).
[31] Law Council of Australia, Submission to the Senate Legal and Constitutional Affairs Committee, *Telecommunications Amendment (Get a Warrant) Bill 2013* (31 July 2018).
[32] Inspector-General of Intelligence and Security, *2017-2018 Annual Report* (14 September 2018), available online https://www.igis.gov.au/sites/default/files/files/IGIS%20Annual%20Report%202017-2018%20PDF%201_7MB.pdf.

Recommendations

- **The Review should consider recommending a comprehending revision of the TIA Act, with for example urgent amendments to:**
  - **introduce defined limits on the issue of B-party warrants and the derivative use of material collected by a B-party warrant;**
  - **increase the penalty thresholds for stored communications warrants to apply only to criminal offences; and**
  - **increase the threshold for sharing stored communications to that prescribed in sections 110 and 139 of the TIA Act.[33]**
- **A comprehensive review of the TIA Act should also consider the need for judicial warrant for access to telecommunications data.**
- **The Review consider legislative amendments that introduce a greater level of oversight and accountability into the existing regime for authorising access to and disclosure of telecommunication data by certain enforcement and intelligence agencies. This may include replacing a system of authorisations for accessing and disclosing prospective telecommunications data with a warrant-based system.[34]**

Secrecy offences and unauthorised access to sensitive information

66. The Law Council remains concerned with regard to the framing of secrecy offences across the legislation relating to the AIC agencies, the AFP, ACIC, AUSTRAC and the Department of Home Affairs. The Law Council is of the view that there is a need for implementation of key recommendations arising from the ALRC's Secrecy Report to ensure that such offences are proportionate. Several of the current provisions do not appear to meet the standards set by the Secrecy Report. In the Secrecy Report, the ALRC generally:

    - recommended that a general secrecy offence be established for behaviour that harms, is reasonably likely to harm or intended to harm, essential public interests;
    - accepted that harm was implicit in any disclosure of information obtained or generated by intelligence agencies;
    - accepted that specific secrecy offences could be justified in this context (the ALRC recommended that many secrecy offences be abolished and a new general secrecy offence be created);
    - recognised in this context a distinction between secrecy offences directed specifically at insiders (who have special duties to maintain secrecy) and those capable of applying to all persons; and

[33] See the Law Council of Australia Submission to the Senate Standing Committee on Legal and Constitutional Affairs *Comprehensive Review of the Telecommunications (Interception and Access) Act 1979* (14 March 2014).
[34] Law Council of Australia, Submission to the Senate Legal and Constitutional Affairs Committee, *Telecommunications Amendment (Get a Warrant) Bill 2013* (31 July 2018).

- recommended that secrecy offences capable of applying to persons other than insiders have an express harm requirement.[35]

67. These principles were recently affirmed by the second INSLM in his *Report on the impact on journalists of section 35P of the ASIO Act*.[36] The second INSLM made recommendations regarding the specific secrecy offence relating to special intelligence operations which were subsequently adopted through amendments to the provision.[37]

68. While some of these principles appear to have been followed in the drafting of the secrecy offences for example in the EFI Bill, a number of ALRC recommendations remain outstanding:

    - The categories of 'inherently harmful information' and 'causing harm to Australia's interests' do not accord with the harmful behaviour identified by the ALRC;

    - In the absence of an express harm requirement secrecy offences should cascade in penalty and require that a person knew, or as a lesser offence, was reckless as to whether, the protected information falls within a particular category (i.e. security classification or concerns Australia's national security), and should not provide that strict liability applies to that circumstance.

    - There should be a public interest defence, rather than a 'journalist' defence which includes the term 'news media', the meaning of which is uncertain. The Law Council is opposed to the notion that the public interest exception should only be available to journalists or the news media. This is not a proper criterion for criminal liability. A person who supplied information (e.g. about malpractice in the prosecution process) to a journalist would have no defence but the person who reported it in the news media would have a defence. The defence refers to news media but it is not clear that it would, for example, pick up individual blogging. The policy of punishing those who deal with such information outside the news media also requires justification.

69. The Law Council also maintains the concerns regarding the secrecy offences, as outlined in our submissions to the PJCIS,[38] that the definition of 'cause harm to Australia's interest' under section 121.1(1)(a) – 'interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth' – remains concerning. 'Interfere with' remains very broad and may well stifle criticism of police, security or prosecution officials who have acted improperly or negligently.

70. Adequate exemptions should always be provided to preserve client legal privilege and the confidentiality between a lawyer and their client.

---

[35] See also Independent National Security Legislation Monitor The Hon Roger Gyles AO QC, *Certain questioning and detention powers in relation to terrorism* (October 2016), 18.
[36] Independent National Security Legislation Monitor The Hon Roger Gyles AO QC, *Certain questioning and detention powers in relation to terrorism* (October 2016), 18.
[37] Ibid 23.
[38] Law Council of Australia, Submission No 5 to the Parliamentary Joint Committee on Intelligence and Security, *National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (22 January 2018).

Recommendations

- **The outstanding recommendations of the ALRC's Secrecy Report should be implemented, including:**
  - **The general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to:**
    - **damage the security, defence or international relations of the Commonwealth;**
    - **prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;**
    - **endanger the life or physical safety of any person; or**
    - **prejudice the protection of public safety.**
  - **In the absence of an express harm requirement secrecy offences should cascade in penalty and require that a person knew, or as a lesser offence, was reckless as to whether, the protected information falls within a particular category (i.e. security classification or concerns Australia's national security), and should not provide that strict liability applies to that circumstance.**
  - **There should be a public interest defence, rather than a 'journalist' defence which includes the term 'news media', the meaning of which is uncertain.**
- **Adequate exemptions should always be provided to preserve client legal privilege and the confidentiality between a lawyer and their client.**

Requirement of all ISA agencies to seek a Ministerial Authorisation for activities likely to have a direct effect on an Australian person

71. The IRR made the following recommendation 16(c):

> *Introducing a requirement for all ISA agencies to seek a Ministerial Authorisation for activities likely to have a direct effect on an Australian person.*

72. Currently the responsible Ministers in relation to ASIS, AGO and ASD must each issue a written direction under subsection 8(1) of the ISA to the relevant agency head. The direction must require the agency to obtain an authorisation under section 9, 9A or 9B (as the case requires) before undertaking, in accordance with a direction under paragraph 6(1)(e), an activity, or a series of activities, that will, or is likely to, have a direct effect on an Australian person (sub-paragraph 8(1)(a)(ii) of the ISA). Paragraph 6(1)(e) relates to a function of ASIS to undertake such other activities as the responsible Minister directs relating to the capabilities, intentions or activities of people or organisations outside Australia.

73. The Law Council considers that implementation of Recommendation 16(c) would provide an important accountability safeguard where activities of ISA agencies (other than ASIS) are likely to have a direct effect on an Australian. This is particularly important if other recommendations of the Review are to be implemented which would allow ISA agencies more broadly to seek class authorisations and to streamline cooperation provisions.

74. The Law Council would be pleased to consider other specific proposals for reform if these are articulated.

Recommendation

- **Recommendation 16(c) of the IIR be implemented:**
  Introducing a requirement for all ISA agencies to seek a Ministerial Authorisation for activities likely to have a direct effect on an Australian person.

Compulsory questioning framework

75. The Law Council welcomed the PJCIS's recommendation in March 2018 regarding its inquiry into ASIO's questioning and detention powers that the Government develop legislation for a reformed ASIO compulsory questioning framework, and refer this legislation to the PJCIS for inquiry and report.[39] The Law Council understands that the Australian Government is currently developing legislation to revise ASIO compulsory questioning powers. The Law Council welcomes a removal of ASIO's current questioning and detention power as consistent with its own recommendations and those of the first and second INSLMs and the PJCIS. The Law Council considers that the framework should be similar to the framework for the ACIC with appropriate modifications in place.

76. The Law Council also maintains its position that:

- The examination of an accused person by ASIO and the ACIC should be deferred until after the disposition of any charges. In the alternative, the ASIO Act and ACC Act should require authorisation from a Federal Court judge before a summons is issued to a person who is subject to criminal proceedings, and for that Judge to prescribe limitations on the matters which may be covered by the examination.
- The ACC Act and any ACIC model adapted to ASIO's questioning and detention powers should require the existence of an earlier compulsory examination to be a factor to be taken into account by the issuing authority and the examiner (the one person) if the recommendations as to questioning warrants (**QWs**) are implemented, accompanied by a register of examinees to be kept and shared with the bodies concerned.

Recommendations:

- **The examination of an accused person by ASIO and the ACIC should be deferred until after the disposition of any charges.**
- **In the alternative, the ASIO Act and ACC Act should require authorisation from a Federal Court judge before a summons is issued to a person who is subject to criminal proceedings, and for that Judge to prescribe limitations on the matters which may be covered by the examination.**

[39] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *ASIO's questioning and detention powers* (2018), xi.

National Security Information (Criminal and Civil Proceedings) Act 2004

77. The Law Council remains deeply concerned regarding certain provisions of the *National Security Information (Criminal and Civil Proceedings) Act 2004 (***NSI Act**) and the potential for operation of the provisions to result in an abuse of process. For example, Law Council remains concerned that a subject of a control order or their legal representative may not have access to information used against them in a control order proceeding. While the Law Council is pleased that there is now a system of special advocates for control order proceedings, this is no replacement for access to information by a client's legal representative.

78. The special advocate regime must include a minimum set of standards that addresses difficulties encountered with such schemes in other comparable overseas jurisdictions. For example, practical support must be available and adequate funding should be provided without burdening existing legal aid funding.

79. The appointment of the special advocate should be a last resort, where the trial judge is satisfied that no other alternative will adequately meet the interests of fairness to the affected individual.

80. The Law Council has previously raised a range of concerns[40] with these provisions, including concerns that:

    (a) The notification provisions are unworkable and too broad. They place a heavy burden on parties and lawyers engaged in federal proceedings as well as the Attorney-General and are not necessary in light of pre-existing options for protecting national security information in court proceedings;

    (b) The security clearance system for lawyers under sections 39 and 39A of the NSI Act threatens the right to a fair trial by:

        (i) potentially restricting a person's right to a legal representative of his or her choosing by limiting the pool of lawyers who are permitted to act in cases involving classified or security sensitive information; and

        (ii) potentially allowing the executive arm of government to effectively 'vet' and limit the class of lawyers who are able to act in matters which involve, or which might involve, classified or security sensitive information;

    (c) The court's discretion to maintain, modify or remove restrictions on disclosure of information is unduly fettered;

    (d) Although the more intrusive features of the NSI Act have been used infrequently, the existence of these provisions continue to cast a shadow over the expedient and fair conduct of proceedings, particularly terrorism related criminal proceedings, and if triggered, threaten to undermine the defendant's right to a fair trial and the independence of the legal profession;

    (e) The security clearance requirements for legal practitioners continue to be intrusive, disruptive to proceedings and unnecessary in light of other obligations on legal practitioners and other mechanisms for protecting security information.

[40] Law Council of Australia, Submission to the Independent National Security Legislation Monitor Bret Walker SC, *Inquiry into the operation of the National Security Information (Criminal and Civil Proceedings) Act 2004* (19 July 2013).

(f) The notification provisions in the Act create a time-consuming set of obligations on each of the parties and the Attorney-General. These requirements in turn lead to delay and disturbance to the trial process, including the possibility of a disruption to the trial itself; and

(g) The need for the system of non-disclosure and witness exclusion certificates, in conjunction with the onerous notification requirements, remains unsubstantiated particularly when regard is had to the pre-existing mechanisms for protecting national security information.

81. For these reasons, the Law Council maintains its recommendations made in its submission to the INSLM, namely that:

- defendants and their legal representatives could only be excluded from hearings in limited specified circumstances, and that courts would retain the power to stay proceedings if the defendant could not be assured of a fair trial;[41]
- when making an order allowing information to be disclosed subject to the Attorney-General's non-disclosure certificate, the court should be satisfied that any amended document and/or substitution documentation to be adduced as evidence would provide the defendant with substantially the same ability to make his or her defence as would disclosure of the source document;[42]
- when making an order to exclude a witness from the proceedings, the court should be satisfied that the exclusion of the witness would not impair the ability of the defendant to make his or her defence;[43][72]
- sections 39 and 39A of the NSI in relation to the security clearance process be repealed;
- In the alternative, the Law Council recommends that sections 39 and 39A be amended so as to give the court a greater role in both determining whether a notice should be issued and in reviewing a decision to refuse a legal representative a security clearance. A similar recommendation was made by the Senate Committee on Legal and Constitutional Affairs during its inquiries into the NSI 2004 Bills and the NSI 2005 Bill where it recommended that 'the court assume a more active role in determining whether a defendant's legal representative requires a security clearance before he or she can access information'.[44]

82. The Law Council submits that the outstanding recommendations of the INSLM in his third annual report should be addressed, for the reasons outlined in the INSLM's report.[45]

Recommendations

- **In relation to the *National Security Information (Criminal and Civil Proceedings) Act 2004,* the Review consider making the following recommendations:**

[41] Senate Committee on Legal and Constitutional Affairs Report on the Provisions of the *National Security Information (Criminal Proceedings) Bill 2004 and the National Security Information (Criminal Proceedings) (Consequential amendments) Bill 2004* (19 August 2004) Recommendation 1.
[42] Ibid Recommendation 7.
[43] Ibid Recommendation 8.
[44] Recommendation 10.
[45] Independent National Security Monitor Bret Walker SC, *Annual Report* (7 November 2013), 124-155.

- **defendants and their legal representatives could only be excluded from hearings in limited specified circumstances, and that courts would retain the power to stay proceedings if the defendant could not be assured of a fair trial;[46]**

- **when making an order allowing information to be disclosed subject to the Attorney-General's non-disclosure certificate, the court should be satisfied that any amended document and/or substitution documentation to be adduced as evidence would provide the defendant with substantially the same ability to make his or her defence as would disclosure of the source document;[47]**

- **when making an order to exclude a witness from the proceedings, the court should be satisfied that the exclusion of the witness would not impair the ability of the defendant to make his or her defence;[48][72]**

- **sections 39 and 39A of the NSI in relation to the security clearance process be repealed;**

- **In the alternative, the Law Council recommends that sections 39 and 39A be amended so as to give the court a greater role in both determining whether a notice should be issued and in reviewing a decision to refuse a legal representative a security clearance.**

- **the outstanding recommendations of the INSLM in his third annual report should be addressed, for the reasons outlined in the INSLM's report.[49]**

Definition of intelligence activities

83. The ISA states the functions of Australia's national intelligence agencies are to be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic wellbeing, and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.[50]

84. The Criminal Code defines national security as Australia's or a foreign country's political, military, or economic relations with another country or countries.[51]

85. The Law Council is concerned that the extension of intelligence agencies' functions so that the performance of their functions include functions in the interests of Australia's national economic wellbeing, and the inclusion of a foreign country's economic relations in the definition of national security, may allow the powers of the national intelligence agency's powers to be used on a wide range of issues that are disproportionate to their purpose.

---

[46] Senate Committee on Legal and Constitutional Affairs Report on the Provisions of the *National Security Information (Criminal Proceedings) Bill 2004 and the National Security Information (Criminal Proceedings) (Consequential amendments) Bill 2004* (19 August 2004) Recommendation 1.
[47] Ibid Recommendation 7.
[48] Ibid Recommendation 8.
[49] Independent National Security Monitor Bret Walker SC, *Annual Report* (7 November 2013), 124-155.
[50] *Intelligence Services Act 2001* (Cth) s 11(1).
[51] *Criminal Code Act 1995* (Cth).

86. Economic relations or interests may cover a wide range of activity, such as any form of consultancy with a foreign government, the sort that accountancy or legal firms may engage in as a matter of course.

87. Further, it is unclear how 'economic interests' or 'economic relations' is defined, as views as to what is in Australia's economic interests may vary substantially. This may have a stifling effect on freedom of expression, and could have a chilling effect on the discussion of economic ideas.

88. The Law Council therefore recommends that the Criminal Code the ISA and be amended to exclude economic relations from the definition of national security, and Australia's national economic wellbeing from the purpose of an intelligence agency's functions.

Recommendation

- **The Criminal Code and the ISA and be amended to exclude economic relations from the definition of national security, and Australia's national economic wellbeing from the purpose of an intelligence agency's functions.**

Oversight-related legislation

89. The Law Council believes the IGIS, Commonwealth Ombudsman and the INSLM play a critical role in the oversight of Australia's NIC, and continues to be a necessary and effective form of scrutiny of Australia's national security and counter-terrorism legislation.

90. The Law Council recommends that the INSLM Act should be amended as to address the issues raised by the first INLSM Bret Walker SC.[52] Firstly, that there should be an express power for the INSLM to report on a matter or matters within the statutory mandate but more urgently or particularly than by the annual report. The Law Council is concerned, however, that the ability of the INSLM to conduct own motion reports may be hindered by a requirement to respond to referrals by the PJCIS for briefings and reports. Should this recommendation be implemented, the INSLM's office should also be allocated additional resources to fulfil its expanded responsibility.

91. Secondly, that the INSLM Act be amended so there is no possibility of reappointment of the INSLM. Mr Walker noted that:

> *The nature of the task should not only involve quasi-judicial tenure (during the term of appointment) so as to remove fear of the Executive, but there should as well be no hope of preferment from the Executive. As a corollary of this suggested repeal of subsec 12(2) of the INSLM Act and its replacement by a prohibition on reappointment, consideration should be given to the enlargement of the term of office probably to four years and possibly to five years. In turn, this may well reduce the pool of willing appointees considerably.*[53]

92. The Law Council further recommends that the INSLM Act be amended to require the Government to provide a public response to the INSLM's recommendations within six months.

[52] Independent National Security Monitor Bret Walker SC, *Annual Report* (28 March 2014), 2.
[53] Independent National Security Monitor Bret Walker SC, *Annual Report* (28 March 2014), 2-3.

93. The Law Council also notes the importance of adequate resourcing to ensure that statutory office holders such as the IGIS, Ombudsman and INSLM can adequately perform their statutory functions

94. The IGIS has for example expressed the need to ensure adequate resourcing when new legislation and powers are introduced that may be complex and resource intensive.[54] The IGIS noted that the adequacy of resourcing to maintain effective oversight (including complaint management and accessing independent technical expertise) will require ongoing monitoring, including as informed by the frequency and manner of use of the new power by agencies.

95. The Law Council supports the increased oversight role of the PJCIS and the IGIS to all ten agencies within the National Intelligence Community, subject to both bodies being allocated additional resources.

Recommendation

- **The INSLM Act be amended so that:**
  - **there should be an express power for the INSLM to report on a matter or matters within the statutory mandate but more urgently or particularly than by the annual report. If this is accepted;**
  - **there be no possibility of reappointment of the INSLM; and**
  - **the Government be required to provide a public response to the INSLM's recommendations within six months.**
- **The IGIS, Ombudsman and INSLM offices should be allocated additional resources to fulfil any expanded responsibility.**

[54] Inspector-General of Intelligence and Security, Submission No 52 to the Parliamentary Joint Committee on Intelligence and Security, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (12 October 2018) 5-6.