Law Council
OF AUSTRALIA

National Security Legislation Amendment Bill (No. 1) 2014

Parliamentary Joint Committee on Intelligence and Security

6 August 2014

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www lawcouncil asn au

Table of Contents

Acknowledgement

The Law Council acknowledges the assistance of its National Criminal Law Committee, National Human Rights Committee, the New South Wales Law Society and the Law Society of South Australia in the preparation of this submission.

Executive Summary

1. The Law Council acknowledges the serious nature of emerging national security threats and the importance of ensuring that Australia's intelligence community (AIC) is equipped to defend Australians and Australia's national security interests. Effective intelligence capabilities are essential to warning of national security threats, understanding the regional and international environment, military capabilities and intentions of potential adversaries, supporting military operations and foreign, trade and defence policy.[1]

2. The Law Council supports efforts to explore what existing legal mechanisms are available to AIC officials to enable them to effectively perform their vital roles. It recognises that gaps may be identified when evaluating the existing legal framework's capacity to respond to the particular challenges posed by Australians travelling overseas to engage in terrorist related activities and recent mass disclosures of classified intelligence abroad. If gaps are identified, the Law Council urges the Government and the Parliament to ensure that any new laws are only introduced when shown to be necessary and proportionate, having regard to rule of law and human rights principles, and in light of the broad range of exceptional powers which are currently available to address threats to national security.

3. Many features of the National Security Legislation Amendment Bill (No. 1) 2014 (the NSLA Bill) aim to ensure that intelligence agencies are able to effectively perform their functions and cooperate productively given the advances in technology. The Law Council welcomes measures in the NSLA Bill that seek to promote consistency across existing legislative regimes dealing with the powers and functions of intelligence agencies and supports amendments that aim to modernise definitions and to promote efficiency in administrative processes. However, there are many other aspects of this Bill – such as those that seek to significantly expand the existing powers of intelligence agencies without including sufficient safeguards – that raise strong concerns.

4. Both the Law Council and the PJCIS have considered some of the proposals in the Bill in detail. However, many of the features of the Bill have not had the same opportunity for proper Parliamentary scrutiny and public comment. In the short timeframe of the current Parliamentary Joint Committee on Intelligence and Security's (PJCIS) inquiry, the Law Council regrets that it has not had the opportunity to consider in detail a number of proposed measures contained in the NSLA Bill. In this submission, the Law Council has, however, sought to highlight key measures of the NSLA Bill which may require further comprehensive scrutiny and consideration prior to enactment. Where possible, the Law Council has also offered a range of suggestions to ensure that any new measures are accompanied by appropriate safeguards to protect against undue interference with fundamental rights and freedoms, including fair trial rights, the right to privacy and freedom of expression.

5. Four of the measures in the NSLA Bill in particular are worth emphasising:

    - the proposed special intelligence operations (SIO) scheme – the Law Council has strong concerns about the current proposals for a special intelligence operations (SIO) scheme, which would provide for criminal and civil immunity, provided that certain conditions are met, for ASIO officers and other human

[1] Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, 20 July 2004, p 7 at http://www.dpmc.gov.au/publications/intelligence_inquiry/.

sources who become involved in criminal activity during the course of an undercover operation. The Law Council is not convinced of the necessity of such a scheme. If however, the SIO scheme is pursued the Law Council suggests a number of amendments, to enhance accountability. It is important that the SIO scheme does not set a lower standard for controlled operations more generally in Australian jurisdictions, with the likelihood that copycat legislation will follow;

- proposed new offences (and increased penalties for existing offences) concerning unauthorised disclosure or unauthorised dealings with intelligence information. The Law Council notes that the proposed offences or increases in penalties have not been subject to proper consultation despite having the potential for significant limitations on freedom of speech. The proposed offences for unauthorised dealings with, and recording of, intelligence information capture an overly broad range of conduct (for example, they do not require that the unauthorised dealing or recording is likely to considerably harm Australia's national security interests) and are not demonstrated to be necessary;

- certain features of proposals regarding ASIO's warrant powers including the ability of ASIO to access an innocent third-party's computer or an entire computer network or to disrupt such systems to target a suspect. The Law Council makes a number of recommendations to contain the scope of these proposals. While it supports efforts to create consistency across regimes that authorise the use of surveillance devices, it also considers that key safeguards from the *Surveillance Devices Act 2004* (Cth) (the SD Act), which provide a clear transparent approach to determining whether the use of intrusive surveillance devices is necessary and proportionate, should be included in the Bill; and

- amendments which will expand the powers of agencies under the *Intelligence Services Act 2001* (IS Act) to collect intelligence on Australian persons overseas without Ministerial authorization and based on a request by ASIO (which would not, however, be necessary if it was not practicable in the circumstances). The Law Council considers that great care must be taken when seeking to amend the authorisation processes for the use of intrusive intelligence gathering powers. Each Australian intelligence agency has its own clear statutory functions, its own oversight and reporting mechanisms and its own authorisation and warrant processes – all designed to recognise the exceptional nature of these agencies and to provide the parliament and the public with confidence that these agencies are operating within the law. In respect of one of the relevant proposals, the Law Council has recommended that the proposed safeguards should be strengthened. It recommends that another should not be pursued without further clarification and scrutiny.

6. These concerns have led the Law Council to recommend that the NSLA Bill not be passed in its current form and that the PJCIS should request the next appointed Independent National Security Legislation Monitor (INSLM) to consider the operation, effectiveness and implications of existing legislation with a view to addressing the issues which are raised by the Bill[2] While the previous INSLM has considered a few

[2] Under the Independent National Security Legislation Monitor Act 2010 the Monitor can initiate his or her own inquiries into matters relevant to Australia's counter-terrorism and national security legislation in accordance

of the relevant issues (as noted below), most have not been subject to the INSLM's consideration. If this recommendation is not adopted, then the Law Council urges the PJCIS to carefully consider the following recommendations for changes to the Bill that are discussed in detail in this submission.

with section 6 of that Act. The Prime Minister can also refer matters to the Monitor for inquiry (section 7)as can the Parliamentary Joint Committee on Intelligence and Security in more limited circumstances (section 7A).

Summary of Recommendations

7. The Law Council's primary recommendation is that the NSLA Bill not be passed in its current form and that the PJCIS should request the next appointed INSLM to review Australia's existing legislation with a view to addressing the issues which are raised by the Bill.

8. However, if this recommendation is not adopted then the Law Council urges the PJCIS to recommend that the following changes be made to the Bill.

Special Intelligence Operations scheme

9. The Law Council does not support the enactment of a SIO scheme. If such a scheme is pursued, it recommends that the proposed SIO scheme include similar safeguards as those contained in the controlled operations scheme. This would mean amending the proposed SIO provisions to:

    - limit SIOs to only the most significant/ serious intelligence-gathering operations;
    - require an ASIO employee to be involved in an SIO;
    - limit the proposed protections from civil and criminal liability provided under the SIO scheme so that:
        - civil indemnification, rather than immunity, is provided to participants. Provisions should also be included for the Commonwealth to pay compensation in respect of serious property damage or personal injury;
        - participants would not be immune or indemnified from liability if their conduct was *likely to* cause death, serious injury or result in the commission of a sexual offence; and
        - civilians would need to act in accordance with the instructions of an ASIO employee.
    - provide further clarification to ensure that the immunities contained under the proposed SIO scheme do not apply in respect of conduct which is required under a warrant, or regulated by certain provisions of the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) Act;
    - ensure that the provisions for variation of the scheme require that the authorising officer be satisfied of the same criteria applicable during the authorisation process;
    - provide more specific guidance in the authority for the SIO as to its nature and scope, and the conduct to be authorised, including differentiating between the role of civilian participants from ASIO employees; and
    - replace the proposed SIO reporting and oversight mechanisms (which as currently drafted are insufficient) with more stringent measures including: detailed reporting to the Inspector-General of Intelligence and Security (the IGIS) and Minister, clear record-keeping obligations and obligations on the IGIS to regularly inspect and report to the Minister.

10. The Law Council does not support the extension of criminal and civil immunity to civilian participants. If they are, however, to be included in the scheme, it recommends that certain safeguards be included which contain and define the role of civilians in SIOs which are equivalent to the controlled operations scheme (some of which are described above).

11. Further, the Law Council considers that further changes should be made to the proposed SIO scheme to: ensure independent, external authorisation; remove the extension of criminal and civil immunity to civilian (non-ASIO) employees; provide for mandatory review of the scheme after five years; and include a sunset clause.

Offences

12. The Law Council opposes the introduction of offences relating to unauthorised disclosure of an SIO. However, if the proposed offence provisions are pursued, the Law Council recommends that amendments be made to ensure that adequate whistleblower protections are available to ensure freedom of speech is not unduly retrained and that public discussion of important issues of public interest is permissible.

13. .If the new offences in the Bill in respect of unauthorised dealings with, and recording of, intelligence information are, pursued, the Law Council recommends that an additional safeguard be implemented which requires that the unauthorised dealing or recording must be, or be likely to be, prejudicial to national security.

14. If the proposal for an increase in penalties for unauthorised disclosure of sensitive information is pursued, the Law Council recommends that the same safeguard should apply which requires prejudice to national security as a result of the relevant disclosure.

Warrant powers

15. The Law Council recommends that the proposed provisions relating to computer access warrants be amended, where the warrant will provide access to multiple computers, to require a more direct connection between the computer accessed and the nominated person of security interest, and to define key terms such as “computer network”.

16. In respect of surveillance device warrant, the Law Council recommends that the proposed provisions be amended to require an authorising officer to have regard to a similar range of factors as that required under the SD Act part of the authorisation process. Where a single warrant is issued in respect of multiple devices, consideration should be given to ensuring that the use each different device is justified. More specific reporting requirements should also be incorporated relating to the use of surveillance devices.

17. In relation to other proposed changes to the warrant processes in Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* (Cth) (the ASIO Act), the Law Council recommends that:

    (a) the proposed provisions regarding telecommunications in transit and access to third party computers, as well as access to third party premises, should be subject to further limitations on their scope;

    (b) a privacy impact test should be incorporated for the issuing of a warrant under Division 2 of Part III of the ASIO Act. This would require satisfaction that the likely benefit of the access provided under the warrant would substantially outweigh the extent to which the disclosure is likely to interfere with privacy of each person affected;

    (c) the provisions which propose that ASIO personnel, and other persons authorised to exercise warrants on its behalf, may use reasonable and

necessary force should be limited to that recommended by the PJCIS, and not include the use of 'reasonable and necessary force' against persons; and

(d) the proposed power of the Attorney-General to vary warrants, be amended to reflect that the power only applies to amendments of a minor or technical nature; and

(e) clarification be sought as to whether the proposed amendments in relation to the disruption of a computer are intended, as appears to be the case, to permit material interference where necessary for the purposes of executing the warrant.

Changes to the Intelligence Services Act

18. The Law Council recommends that the proposed safeguards included for amendments to the IS Act to enable the Australian Secret Intelligence Service (ASIS), without Ministerial authorization, to cooperate with ASIO in relation to the production of intelligence on an Australian person be strengthened by specifying what kinds of activities could be approved, the length of the approval and the basis on which it could be approved or renewed.

19. The Law Council further considers that the PJCIS should seek further information in order to determine the necessity of the proposed new ground of Ministerial authorization which enables the Minister responsible for ASIS to authorise the production of intelligence on an Australian person who is, or is likely to be, involved in activities that pose a risk to, or are likely to pose a risk to, the operational security to ASIS. It is unclear, for example, why activities which may pose a risk to ASIS' operational security would not fall under the existing authorisation category for 'activities that are, or are likely to be, a threat to security'.

Introduction

20. The Law Council of Australia is grateful for the opportunity to provide the following submission to the PJCIS in response to its inquiry into the NSLA Bill.

21. The primary function of the ASIO Act is to provide a legislative basis for Australia's domestic national security agency, the ASIO. The IS Act provides a legislative basis for Australia's foreign security agencies, including ASIS, the Defence Imagery and Geospatial Organisation (DIGO) and Australian Signals Directorate (ASD). Both pieces of legislation stipulate the functions and powers of the relevant agencies. They are important components of Australia's national security framework defining the parameters of the AIC and seeking to ensure that intelligence collection and analysis can occur only in circumstances designed to benefit and to protect the safety and wellbeing of Australians.

22. The Law Council acknowledges the bipartisan efforts to ensure that proposals to expand or change existing national security laws have been subject to public consultation and review by parliamentary committees including the PJCIS. It notes that a number of the measures contained in the Bill have previously been considered in some detail by this Committee, and the Law Council and other organisations have had the opportunity to provide submissions and raise concerns or suggest further improvements or changes be made.

23. Unfortunately, not all aspects of the Bill have been subject to public consultation or prior scrutiny. Many changes proposed in the Bill that will have significant impacts on the nature and scope of intelligence agencies' powers, and that will in turn impact on the privacy and other rights of ordinary Australians, have not been considered in detail by the PJCIS or other parliamentary committees. The tight timeframes for the present inquiry limits the capacity of the Law Council and other organisations to provide detailed analysis in relation to these proposals.

24. Measures previously suggested by the PJCIS have also not, as recommended by the Committee, been released as an exposure draft for public consultation to allow for a full consideration to ensure that the laws are appropriate and effective.

25. For these reasons, the Law Council urges the PJCIS to make recommendations seeking the views of key stakeholders such as a newly appointed INSLM, who could report on the operation, implications and effectiveness of existing legislation, prior to enactment of the NSLA Bill.

26. Before discussing particular aspects of the NSLA Bill, this submission makes a general comment regarding the ASIO Guidelines. Where the submission refers to a PJCIS recommendation, it should be noted that this is a recommendation from the PJCIS's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* of May 2013 (PJCIS Report) unless otherwise specified.

General Comment – ASIO Guidelines

27. Pursuant to subsection 8A(1) of the ASIO Act the Attorney General can issue Guidelines that are to be observed by ASIO in the performance of its functions of obtaining, correlating, evaluating and communicating intelligence relevant to security and provide important instruction on when and how existing powers, conferred under the ASIO Act, may be exercised.

28. As explained on ASIO's website,[3] the Guidelines do not broaden ASIO's powers beyond the ASIO Act. The Guidelines set some parameters around the conduct of ASIO's investigations and inquiries.

29. These Guidelines are referred to in the Statement of Compatibility with Human Rights accompanying the NSLA Bill and contain important safeguards to guard against the misuse or overuse of ASIO's powers, including its special powers that are subject to amendments in this Bill. For example, the Guidelines provide that :

    - in the conduct of its inquiries and investigations, ASIO must ensure that the means used to obtain information are proportionate to the gravity of the threat posed and the probability of its occurrence. The more intrusive the investigation technique, the higher the level of officer required approving its use and wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.

    - in conducting inquiries and investigations into individuals and groups, ASIO should do so with as little intrusion into individual privacy as is possible consistent with the performance of its functions, with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest.

30. If the amendments proposed in the NSLA Bill are enacted, these Guidelines will be critical to ensuring that the expansive, covert and intrusive powers available to ASIO are exercised only when necessary and proportionate and having regard to the impact on the rights of individuals subject to ASIO's inquiries or investigations.

31. When evaluating the amendments proposed in the NSLA Bill, the Law Council encourages the Committee to have regard to these Guidelines and recommends that that:

    (a) the Guidelines be reviewed by both the IGIS and the INSLM having regard to the issues raised in the Bill – including their application in relation to ASIO affiliates as well as ASIO employees - noting that the Guidelines do not appear to have been amended since 2008;

    (b) section 8A of the ASIO be amended to provide a mechanism to promote compliance with these Guidelines;

    (c) the IGIS Act be amended to specifically require that the IGIS review the Guidelines on a regular basis;

    (d) the Guidelines be amended having regard to the relevant recommendations of the Australian Law Reform Commission's (ALRC) 2008 report *For Your Information: Australian Privacy and Practice* (ALRC Report 108) into the protection of privacy in Australia which contained some recommendations relevant to the application of the ASIO Guidelines. For example, the ALRC recommended that:

        (i) the privacy rules and guidelines that relate to the handling of intelligence information concerning Australians by ASIO should be amended to include consistent rules and guidelines relating to: the handling of personal information about non-Australian individuals, to the extent that

[3] See http://www.asio.gov.au/About-ASIO/Oversight-and-Accountability/Attorney-General-Guidelines.html.

this is covered by the *Privacy Act 1988* (Cth); incidents involving the incorrect use and disclosure of personal information (including a requirement to contact the Inspector-General of Intelligence and Security and advise of incidents and measures taken to protect the privacy of the individual); the accuracy of personal information; and the storage and security of personal information; and

(ii) section 8A of the ASIO Act be should be amended to require that the: guidelines issued by the Minister include guidelines regulating the handling of intelligence information about individuals by ASIO, (except where ASIO is engaged in activity outside Australia and the external territories; and that activity does not involve the handling of personal information about an Australian citizen or a person whose continued presence in Australia or a territory is not subject to a limitation as to time imposed by law); and the Minister responsible for ASIO consult with the Director-General of Security (the DG), the Privacy Commissioner, the IGIS and the Minister responsible for administering the Privacy Act before making privacy guidelines about the handling of intelligence information.

32. These general comments relating to the Guidelines are particularly relevant to the reforms proposed in Schedule 2 relating to computer access warrants, surveillance device warrants, foreign intelligence warrants and security intelligence warrants.

Schedule 1 – ASIO Act employment provisions

33. Schedule 1 of the NSLA Bill seeks to modernise the ASIO Act employment provisions to more closely align them with Australian Public Service (APS) standards, streamline and simplify terminology used to describe employment and other relationships and make consequential amendments to a range of other Acts.

34. The NSLA Bill for example provides for the secondment of staff to and from ASIO and facilitating the transfer of ASIO employees to APS agencies while protecting their identity.

Secondment Arrangements

35. Some of the measures contained in Schedule 1 seek to implement PJCIS Recommendation 26, namely that the ASIO Act be amended to modernise the Act's provisions regarding secondment arrangements.

36. New sections 86 and 87 seek to provide an express secondment mechanism within the ASIO Act for the secondment of ASIO employees and the secondment of persons to ASIO respectively. Under new sections 86 and 87 a seconded staff member will carry out only the functions of the host organisation in accordance with any procedures or restrictions that apply under legislation to the host organisation.

37. The Law Council expects that other organisations (including those agencies with direct experience with secondments) would be best placed to respond to this reform.

38. However, if the secondment proposal is adopted, amendments must enable, as the IGIS has noted, secondments to reflect a true change in working arrangements for a

reasonable period.[4] It is not appropriate for such a mechanism to be used to circumvent limits placed on employees in other legislation (for example, it would not be proper for an ASIS staff member to be seconded to ASIO for a day or two to enable them to perform an activity that they would otherwise not be permitted to undertake).

39. The Law Council notes that under the legislative proposals the secondment arrangement would be determined on a case-by-case basis. There is no requirement for a minimum or reasonable period to be served as suggested by the IGIS.

40. The Law Council recommends that new sections 86 and 87 be amended to provide that secondments must be for a minimum reasonable period. Alternatively, the Ministerial Guidelines under section 8A of the ASIO Act should include such measures for secondment arrangements.

41. Further, the Law Council recommends that the secondment arrangements be subject to IGIS oversight and that the IGIS be required to regularly review and report on secondment arrangements in the IGIS's annual report and on a confidential basis to the Attorney-General. The IGIS should be given additional resources to review such arrangements. While new subsection 8(8) of the IGIS Act will allow the IGIS to inquire into a matter to which a complaint to the IGIS is made (for example by an ASIO affiliate as it relates to a contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for ASIO or the performance of functions or services by the ASIO affiliate under the contract, agreement or other arrangement), the legislative amendments do not require the IGIS to regularly review the effectiveness of secondment arrangements or report on these for instance in the IGIS's annual report.

ASIO employee powers, responsibilities and duties to be undertaken by ASIO affiliates

42. The Law Council considers that there are a number of new changes relating to employment provisions that have not yet had the opportunity for proper scrutiny or review.

43. Schedule 1 of the Bill creates two new categories an 'ASIO employee' and an 'ASIO affiliate'. It also makes a number of changes to various pieces of legislation substituting an 'officer or employee of ASIO' with an ASIO employee or an ASIO affiliate.

44. Further, the current definition of a 'senior officer of the Organisation' is also substituted by a 'senior position-holder' which is defined as meaning an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee or a position known as Coordinator.

45. The Explanatory Memorandum to the Bill notes that these are 'minor or technical amendments and do not have any human rights implications'.

46. However, in the Law Council's view the amendments do not simply appear to be minor or technical – as suggested by the Explanatory Memorandum – but increase the number of people able to perform duties and functions and exercise powers currently only permitted to be carried out by an officer or employee of ASIO.

[4] IGIS submission to the PJCIS's Inquiry into potential reforms of National Security Legislation, 23 August 2012.

47. For example:

- section 7 of the TIA Act outlines the circumstances in which a person is prohibited from intercepting a communication passing over a telecommunications system. Paragraph 7(2)(ac) provides an exception to section 7 and provides that the prohibition does not apply in relation to the interception of a communication where the interception results from, or is incidental to, action taken by an officer of the Organisation, in the lawful performance of his or her duties' for certain purposes. Item 60 of the Bill amends paragraph amends paragraph 7(2)(ac) to omit 'officer of the Organisation' and substitute 'ASIO employee'. In addition, Item 61 of the Bill inserts a new paragraph 7(2)(ad) after paragraph 7(2)(ac) to provide that section 7 does not apply in relation to the interception of a communication where the interception results from, or is incidental to, action taken by an ASIO affiliate, in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation, for the purpose of:

  - discovering whether a listening device is being used at, or in relation to, a particular place, or

  - determining the location of a listening device;

- item 64 will amend subsection 18(4) of the TIA Act to provide that a written certificate signed by the DG or the Deputy DG may set out matters with respect to anything done by an ASIO employee or an ASIO affiliate with the execution of a warrant. Currently, subsection 18(4) refers to an officer or employee of ASIO.

- item 70 will allow the DG to communicate foreign intelligence information to an ASIO employee or ASIO affiliate under the TIA Act. Item 71 will allow the DG or an ASIO employee or ASIO affiliate to receive foreign intelligence information from another ASIO employee or ASIO affiliate. Item 72 provides that the DG or an ASIO employee or ASIO affiliate may make use of, or make a record of, foreign intelligence information under the TIA Act. Currently, all of the relevant existing provisions refer to an officer or employee of ASIO.[5]

- the amendments also expand the immunity of ASIO affiliates from prosecution. For example, Item 69 of the Bill inserts a new paragraph 108(2)(ga) after paragraph 108(2)(g) to provide that the offence in subsection 108(1) of the TIA Act does not apply in relation to accessing a stored communication if the access result from, or is incidental to, action taken by an ASIO affiliate etc. The SD Act will also be amended to provide that the offences in section 45 (on the use, recording, communication or publication of protected information or its admission in evidence) do not apply to the use, recording or communication of protected information by an ASIO employee or an ASIO affiliate.

- the *Public Interest Disclosure Act 2013* (Cth) will also be amended to the effect that a Commonwealth employee cannot disclose information relating to the identity of an ASIO employee or ASIO affiliate.

[5] Subsections 136(2)(3) and (4) of the TIA Act.

48. Given that the Law Council has had only limited time to review these provisions, it recommends that the PJCIS seek further information relating to Part 2 of Schedule 1, with a view to clarifying:

    - how the proposed amendments expand the ability of individuals other than ASIO employees to utilise significant powers and protections;
    - which kinds of people are covered under these amendments, the types of services they provide to ASIO and under what arrangements; and
    - what arrangements will be in place to ensure that such individuals have the professional skills, conduct and ethics and are able to be held accountable to undertake each of the specific functions and duties which are currently limited to ASIO employees.

Schedule 2 - Expansion of ASIO's warrant based intelligence powers

49. Schedule 2 of the Bill seeks to implement the PJCIS's Recommendations 20 to 23, 29 to 32 and 35 and 36 by streamlining and improving the warrant provisions in Division 2 of Part III of the ASIO Act (which relates to ASIO's special powers). A number of the measures contained in this Schedule are considered below.

Computer access warrants

Enabling ASIO to obtain intelligence from a number of computers (including a computer network) under a single computer access warrant

50. Schedule 2 seeks to enable ASIO to obtain intelligence from a number of computers (including a computer network) under a single computer access warrant, including computers at a specified location or those which are associated with a specified person. In this respect, the Schedule seeks to implement the PJCIS's Recommendations 20.

51. In PJCIS Recommendation 20 the Committee recommended that the definition of computer in the ASIO Act be amended by adding to the existing definition the words 'and includes multiple computers operating in a network'. The Committee further recommended that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.

52. Item 4 of the Schedule extends the definition of 'computer' to include to 'computer networks' and makes it clear that the definition of 'computer' under the ASIO Act, means all, or part of, or any combination of, one or more computers, computer systems and computer networks.

53. Item 18 of the NSLA Bill amends section 25A of the ASIO Act to enable the target computer of a computer access warrant to include any one or more of the following:

    - a particular computer or computers specified in the warrant,
    - computers on particular premises specified in the warrant; or
    - computers associated with, used or likely to be used by a person specified in the warrant, whose identity may or may not be known.

54. For the first two of these categories - relating to a 'a particular computer' and 'a computer on particular premises' - there is no proposed requirement that it be associated with a person.

55. A 'computer on a particular premises' given the proposed definition of computer is also very broad. 'Premises' is defined under section 22 of the ASIO Act to include any land, place, vehicle, or aircraft. It could include, for example, include a head office in which thousands of people are employed.

56. In addition, the Law Council is concerned that there is currently no definition of a 'computer network'. In this respect, the Law Council notes that its own staff use computers on occasion through a remote access network which can be accessed from their homes. Using this example, it is unclear whether the information on staff's home computers would be covered as part of the warrant in respect of a 'computer network'.

57. The Law Council understands the need to ensure that processes associated with computer access warrants are efficient. However, the Law Council considers that in order to protect privacy rights from undue intrusion, access to computers should be on the basis that there is a demonstrated sufficient nexus between the computers accessed and the nominated person of security interest. Rule of law principles also demand that there is greater clarity as to the scope of conduct which will be permissible under the warrant.

58. For example, ASIO should not be able to seek a warrant to access the computers on a particular network, or at a nominated location unless there are reasonable grounds to believe that the person in relation to whom intelligence is being sought had a direct connection with computers other than his/her own on the network.

59. Further, it is suggested that the likely benefit to the investigation which would result from the access to the broader network or computers at a nominated location should substantially outweigh the extent to which the access is likely to interfere with the privacy of any person or persons.

60. It is also suggested that consideration be given to defining key terms such as 'network'.

Allowing ASIO to use a communication in transit to access a target computer under a computer access warrant

61. Item 23 of the Bill inserts new paragraph 25A(4)(ab) that amends the existing power found under current paragraph 25A(4)(a) to use a third party computer, and adds the new power to use a communication in transit for the purpose of obtaining access to data relevant to the security matter and held on the target computer. ASIO may only do so where it is reasonable in all the circumstances, having regard to other methods of obtaining access to the data which are likely to be as effective. ASIO will not be able to use third party computers or communications in transit for any other purpose.

62. A 'communication in transit' will be defined by a new section 22 as a 'communication (within the meaning of the Telecommunications Act 1997) passing over a telecommunications network (within the meaning of that Act)'.

63. As noted in the Explanatory Memorandum to the NSLA Bill (page 63), this measure seeks to ensure that a computer access warrant can capture a broad range of electronic communication that may take place in the modern communications environment (for example, emails passing over a wi-fi network).

64. This measure also seeks to implement PJCIS Recommendation 22 that the Government amend the warrant provisions of the ASIO Act to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant.

65. However, Item 23 is not subject to the appropriate safeguards and accountability mechanisms which were recommended by PJCIS's Recommendation 22, namely those that apply under existing provisions under the TIA Act such as subsection 9(3). Those safeguards provide that the Attorney-General must not issue the relevant warrant unless he or she is satisfied that ASIO has exhausted all other practicable methods or where it would not otherwise be possible to intercept the relevant communications. The PJCIS also referred to the IGIS suggestions that the impact on the third party including his/her privacy must be considered carefully in the approval process.

66. Allowing ASIO to use a communication in transit to access a target computer under a computer access warrant is a significant expansion of power with serious privacy implications. If such powers can be shown to be necessary, appropriate safeguards and accountability mechanisms must be included that acknowledge the serious privacy implications arising from powers to access the computers and communications of innocent third parities.

67. The proposed amendments include safeguards of requiring: access to a communication in transit or a third party computer to be reasonable in the circumstances; and the Minister is only to issue the warrant if he or she is satisfied that there are reasonable grounds for believing that access by the Organisation to data held in a computer (the *target computer*) will substantially assist the collection of intelligence in accordance with this Act in respect of a matter (the *security matter*) that is important in relation to security.[6] In addition, under new subsection 33(1) ASIO will not be permitted under new section 25A to intercept a communication passing over a telecommunications system operated by a carrier or carriage service provider, within the meaning of the TIA Act, unless it has applied for a warrant under the TIA Act (unless otherwise exempted under the TIA Act).

68. The Law Council considers that these safeguards should be strengthened to incorporate the safeguards suggested by PJCIS Recommendation 22 and require that the Attorney-General must not issue the relevant warrant unless he or she is satisfied that ASIO has exhausted all other practicable methods or where it would not otherwise be possible to intercept the relevant communications.

69. In past submissions in respect of the use of covert interception powers under the TIA Act the Law Council has recommended that a single, privacy impact test be included as part of the warrant processes. A similar recommendation can be made in respect of these proposed amendments to the ASIO Act.

70. The single privacy impact test proposed by the Law Council would require issuing authorities, before authorising the use of a computer access warrant and any other warrant under Division 2 of Part III of the ASIO Act to:

- consider whether the use of the access would be likely to deliver a benefit to the investigation or inquiry;

[6] The Law Council notes that the current test for the issue of a computer access warrant would apply albeit with modifications. Item 16 of the NSLA Bill amends subsection 25A(2) by removing the word, 'particular' before computer from subsection 25A(2).

- consider the extent to which the use of the access is likely to interfere with the privacy of any person or persons; and

- be satisfied on reasonable grounds that the likely benefit to the investigation which would result from the access to the communication or third party computer substantially outweighs the extent to which the disclosure is likely to interfere with the privacy of each person or persons.

71. Legislation should also expressly provide that such a warrant is not permitted to authorise ASIO to obtain intelligence material not related to the purpose of the warrant from the third party computer or the communication in transit.

Allowing ASIO to disrupt a target computer

72. Currently, paragraphs 25(5)(a) and 25A(4)(a) provides that the powers under an ASIO search warrant or computer access warrant respectively may include the power to add, delete or alter other data (that is not relevant to the security matter) in a computer or other electronic equipment, or data storage device, where doing so is necessary for the purpose of obtaining access to data that is relevant to the security matter. Items 11 and 22 of the Bill will also provide the power to copy such data.

73. ASIO is not permitted under an ASIO search warrant or a computer access warrant to add, delete or alter data, or do any thing, that interferes with, interrupts or obstructs the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises, or that causes any loss or damage to other persons lawfully using the computer, equipment or device (subsections 25(6) and 25A(5)).

74. Schedule 2 will amend this current limitation on disruption of a target computer in subsections 25(6) and 25A(5) and section 25A to allow ASIO to add, copy, delete or alter data if it is necessary to do one or more of the things specified in the warrant.

75. For example, under new proposed subsection 25(6) (which relates to a search warrant), it provides that subsection 25(5) (which sets out the things that the Minister may specify in the warrant) is not available in respect of the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

    (a) materially interfere with, interrupt or obstruct the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified under subsection (5); or

    (b) cause any other material loss or damage to other persons lawfully using the computer, equipment or device.[7]

76. This will allow ASIO to manipulate a target's computer, for example, by planting malware on a computer in order to more effectively monitor a target.

77. These measures seek to implement PJCIS Recommendation 21 which provides that the Government give further consideration to amending the warrant provisions in the ASIO Act to enable the disruption of a target computer for the purposes of executing

[7] Item 12 of the Bill. A similar replacement provision is provided in respect of subsection 24A(5) (which relates to computer search warrants) at item 25.

a computer access warrant but only to the extent of a demonstrated necessity. The Committee further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.

78. The Law Council recognises the need to ensure that ASIO can covertly access computers in certain limited circumstances where necessary for the performance of its functions.

79. The Law Council acknowledges that ASIO should be able to cause a very minor disruption – for example a temporary slowing of the computer – for the purposes of enacting a warrant. It is unclear whether existing paragraph 25A provides for such a minor disruption given the subsection 25A(6) exception.

80. However, the proposed changes could be interpreted as going further than this by permitting a *material* interference if it is for the purposes of the search or computer access warrant (see paragraphs 25(6)(a) and 25A(5)(a)). It refers to material interference not being authorised *unless* it is necessary etc.

81. In addition, the reference in paragraphs 25(6)(b) and 25A(5)(b) to "any other material loss or damage" not being authorised is not clear. For example, is it intended that material loss or damage will be authorised if it occurs as a consequence of the "necessary" material interference under paragraph 25(6)(a) and 25A(5)(a)?

82. The Law Council notes that permitting a material interference does not appear to be the intention of the legislation as noted in the Explanatory Memorandum. That document notes, for instance, that such an amendment allows ASIO to undertake an action under a computer access warrant that is likely to cause *immaterial* interference, interruption or obstruction to a communication in transit or the lawful use of a computer (for example, using a minor amount of bandwidth or storage space) (at paragraph 288 of the EM).

83. As this proposal could directly affect the activities of persons unrelated to security interests, the Law Council recommends that the PJCIS seek clarity on what kind of 'material' interference, loss and damage would be permissible under these provisions.

84. Further, in the Law Council's view, as noted by the IGIS, it is essential that applications for warrants authorising this action be required to clearly justify why it is appropriate to affect any lawful use of the computer (IGIS submission p 20). As noted by the IGIS, the warrant process should also balance the potential consequences of this interference to the individual(s) with the threat to security. There should also be appropriate review and oversight mechanisms with particular attention to the effect of any disruption on third parties. The NSLA Bill does not, contrary to the PJCIS's Recommendation 21, appear to include such safeguards.

<u>Identified person warrants</u>

85. Schedule 2 establishes an identified person warrant for ASIO to utilise multiple warrant powers against an identified person of security concern (new Subdivision G).

86. The Law Council support efforts to improve administrative efficiency. While it holds in-principle concerns with a warrant approach that enables ASIO to request a single warrant specifying multiple (existing) powers against a single target, these concerns are addressed to some degree by the type of safeguards and criteria outlined in the NSLA Bill and previously by the PJCIS in its recommendation 29 which aims to ensure that the agency and issuing officer to consider whether a sufficient case has been made out that would justify the use of each particular power.

87. Under the 'identified person warrants' scheme, the DG will be able to request that the Minister issue a single warrant authorising the exercise of multiple powers (IPWs). The Minister must be satisfied that the person is engaged in, or is reasonably suspected by the DG of being engaged in, or likely to engage in activities prejudicial to security and the issuing of the warrant in relation to the person, will, or is likely to, substantially assist the collection of intelligence relevant to security.

88. The warrant must specifically provide approval for ASIO to do one or more of the following things:

    - access records or things in or on premises or data held on computers;
    - use one or more kinds of surveillance devices and/ or
    - access postal or delivery service articles.

89. The Law Council notes that under the proposal a single issuing process will apply to allow the simultaneous availability of all powers sought under different types of warrants, while retaining the statutory thresholds for the issuing of individual types of warrants. As noted in the Explanatory Memorandum (p 9), separate authorisation requirements will continue to apply to the issuing of these warrants and the exercise of particular powers under them. IPWs will be for a maximum duration of six months and the Minister may impose restrictions or conditions.

90. An IPW scheme seeks to implement PJCIS Recommendation 29 that should the Government proceed with amending the ASIO Act to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants

91. The Explanatory Memorandum notes that powers under these warrants will include inspecting, copying or transcribing records, use of computers or other equipment to access data, associated powers to search for, inspect and copy records and acts reasonably incidental to exercising these powers and acts necessary to conceal the execution of powers under the warrant.

92. Records can only be retained for as long as is reasonable unless the return of such records would be prejudicial to security. Computers can also be accessed where the Minister has approved such powers under the identified person warrant. Under an authority under an IPW for a computer access, similar types of powers apply as they do with a computer access warrant, similarly for an authority under an IPW in relation to surveillance, for the purposes of a surveillance devices warrant. Searches of a person who are on or near premises being searched can also be conducted, and if so, must (if practicable) be conducted by a person of the same sex. Strip searches and body cavity searches are prohibited. The Law Council agrees with the Explanatory Memorandum that these are important human rights safeguards.

93. Two new provisions, sections 27G and 27H, set out the requirements for inspecting a postal or delivery service article under an IPW where the Attorney-General has conditionally approved the use of such powers. The Minister or DG can authorise the exercise of these powers in a particular instance if they are satisfied on reasonable grounds that this would substantially assist in the collection of intelligence relevant to the prejudicial activities of the identified person – for example, when the post is addressed to the person or posted by them. Relevant powers include inspecting and making copies of the articles or their contents.

94. Safeguards in relation to the authorisations to exercise powers under IPWs where conditional approval has been given by the Minister include that the Minister may impose restrictions or conditions, there must be particularisation of the subject premises or target computers, a higher threshold will apply to the issuing of an IPW than for individual warrants, the period for which search powers can be authorised is 90 days and the period under authorisations cannot extend beyond the timeframe of the warrant itself. The time of which entry is permitted must also be specified, if entry to premises is authorised.

95. The Law Council notes that it appears that IPWs will be subject to IGIS oversight. It also notes that IPWs will be subject to the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and* communicating *intelligence relevant to security (including politically motivated violence)* (the Attorney-General's Guidelines), issued under section 8A of the ASIO Act require ASIO, in the conduct of its inquiries and investigations, to ensure that the means used to obtain information are proportionate to the gravity of the threat posed and the probability of its occurrence. The more intrusive the investigation technique, the higher the level of officer required approving its use and wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.

96. The Law Council considers that safeguards for the IPW scheme could be further strengthened by expressly incorporating a consistent single privacy impact test into the relevant legislative provisions which govern the issuing of a warrant under Division 2 of Part III of the ASIO Act (as discussed above).[8]

Surveillance devices warrants (the single surveillance device warrant)

97. Schedule 2 of the Bill proposes new sections to the ASIO Act that relate to the use of surveillance devices by ASIO.

98. This item implements the Government's response to Recommendation 30 of the PJCIS Report, which provides:

> *The Committee recommends that the Australian Security Intelligence Organization Act 1979 be amended to modernise the warrant provisions to align the surveillance device provisions with the Surveillance Devices Act 2004, in particular by optical devices.*

99. Under the provisions proposed by the Bill, surveillance device warrants may be issued in relation to one or more particular persons, particular premises or an object or class of object. They may also be issued in respect of multiple kinds of surveillance devices and in respect of multiple surveillance devices. In issuing these warrants, the Minister must be satisfied that:

- the person or persons is engaged in or is reasonably suspected by the DG of being engaged in, or of being likely to engage in activities prejudicial to security;
- the premises is used, likely to be used or frequented by such a person, or the object or objects are used or worn, or likely to be used or worn by such a

[8] The Law Council acknowledges that there are certain privacy protections contained in Guideline 10 of the ASIO Guidelines. However, it considers that these should be reinforced in the relevant legislation as set out above.

person and that the use of a surveillance device will, or is likely to, assist ASIO in carrying out its functions of obtaining intelligence. The warrant can only be in force for up to the maximum of six months.

100. Under the provisions proposed in the Bill, warrants will set out a range of authorised activities that can be taken in relation to a particular person, particular premises or an object or class of object. This includes the installation, use and maintenance of a surveillance device, entering premises including third party premises, altering objects and surveilling a person. It also sets out the powers of recovery of surveillance devices.

101. Consistent with the SD Act, the new provisions provide for the use of a listening device and an optical surveillance device without a warrant.

102. The Law Council supports efforts to improve consistency across regimes that authorise the use of surveillance devices and recognizes the need to ensure that key definitions such as 'device', 'enhancement equipment', 'identified person warrant' and 'install' are consistent across the SD Act and the ASIO and keep pace with relevant technological change.

103. When seeking to harmonise existing regimes, care must be taken to ensure that the key principles governing the use of surveillance devices are observed by all agencies authorised to use such devices. Some of these are outlined in section 3 of the SD Act.

104. The ASIO Act also currently contains a general prohibition on the use of listening devices and surveillance devices, with particular exceptions.

105. These existing provisions highlight the fact that the use of covert powers by law enforcement and intelligence agencies to record the words or movements of other people should only be available in exceptional circumstances and subject to strict limits and appropriate oversight and reporting requirements.

106. The Law Council welcomes many features of the amendments relating to surveillance device warrants which transport the detailed requirements for matters that should be specified in a warrant application and what a warrant authorises from the SD Act regime into the ASIO Act.

107. However, the Law Council is concerned that some features of the Bill may have the effect of diluting the important safeguards currently incorporated in the SD Act and ASIO Act regimes. It urges the Committee to be satisfied that the changes proposed in Bill consolidate, clarity and strengthen existing safeguards and rather than broadening the range of purposes and categories of officers authorised to utilise these exceptional and intrusive powers.

108. For example, the Law Council is concerned that the proposed new provisions relating to the determination of a surveillance warrant under the ASIO Act do not incorporate the requirements that currently exist under the SD Act. Section 16 of the SD Act requires warrants to be issued by a judicial officer and only when he or she can be satisfied that there are reasonable grounds for the suspicion or belief founding the application for the warrant. When issuing the warrant the judicial officer must also have regard to:

- the nature and gravity of the alleged offence in respect of which the warrant is sought, and

- the extent to which the privacy of any person is likely to be affected, and
- the existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation, and
- the extent to which the information sought to be obtained would assist the investigation, and
- the evidentiary value of any information sought to be obtained, and
- any previous warrant sought or issued under this Part or a corresponding law (if known) in connection with the same offence.

109. These features of the warrant process – which provide a clear, transparent approach to determining whether the use of intrusive surveillance devices is necessary and proportionate in the particular circumstances - are not replicated in the proposed provisions in the Bill. The Law Council recommends that proposed section 26 of the Bill (item 29 of the Bill) be carefully reviewed and amended to incorporate the matters listed in section 16 of the SD Act to which the issuing authority must have regard before authorising the use of a surveillance device. The Law Council also notes that in past submissions relating to warrant processes under the ASIO Act it has called for consideration to be given to requiring judicial authorisation of warrants. If this approach is not adopted, and surveillance device warrants continue to be issued by the Minister, the Law Council suggests that this highlights the need for the range of matters, such as those listed under section 16 of the SD Act, to be incorporated into the warrant process.

110. The Law Council also urges the Committee to carefully consider whether the provisions designed to introduce a single surveillance device warrant (replacing the need for ASIO to obtain multiple surveillance device warrants for the purpose of using surveillance devices against a person who is the subject of an investigation) continue to require appropriate specificity to enable the issuing authority to assess whether the use of each device is necessary in light of other available measures, and to determine its impact on the privacy and other rights of innocent third parties. Under the existing approach, a separate warrant is required for each device, ensuring that the warrant application specifies the need for each particular advice and its connection with ASIO's intelligence gathering functions. It is not clear, for example, how an issuing authority will determine whether a listening device and a tracking device are *both* necessary if both devices are included in a single warrant.

111. Other changes include provisions which make it clear that the identity of a person referred the subject of a surveillance device warrant need not be known in order for the test for issue of warrant to be met. Although the Explanatory Memorandum states that in circumstances where the person's identity may not be known, there would still need to be sufficient intelligence available about the person in order satisfy the test for the issuance of a surveillance device warrant under section 26, it is not clear how in practice the issuing authority would be able to ensure that the relevant thresholds for issuing the warrant have been met.

112. These changes also highlight the need for the warrant processes in the ASIO Act, particularly those relating to the exercise of covert powers, to have regard to the privacy and other rights of innocent third parties who might, for example, have their conversations or movements covertly captured by ASIO. The Law Council recommends that a single, privacy impact test be included as part of these proposed warrant processes (as discussed further above).

113. The Law Council also urges the Committee to carefully consider the proposed new provisions that authorise the use of listening devices and tracking devices by ASIO without a warrant. The existing provisions of the ASIO Act enable the use of listening and tracking devices by an officer, employee or agent of ASIO, for the purposes of the ASIO, if undertaken with the content of the communicator or if used pursuant to a warrant.

114. The proposed new sections 26C and 26D permit an ASIO employee or an ASIO affiliate to use a listening device without a warrant if the communicator provides implied or express consent.

115. These new provisions may have the potential to enable a broader category of people to utilise these highly intrusive devices without a warrant. The Law Council recommends that the PJCIS seek clarification on this issue.

116. It is noted that new section 26F of the ASIO Act will allow the DG to exclude ASIO affiliates from exercising powers under new sections 26C, 26D and 26E (relating to the use of surveillance devices including listening devices, optical devices and a tracking device without a warrant). The Law Council notes that this measure is an important safeguard in ensuring that, while a particular individual, or class of individuals, may be appropriately performing certain functions or services for ASIO, they are not within the categories of persons who can perform ASIO's powers by use of surveillance devices without warrant. However, ASIO affiliates not the subject to a DG determination under section 26F will still be able to exercise such powers.

117. The Law Council also urges the Committee to recommend that, in addition to ensuring consistency of warrant authorisation processes for the use of surveillance devices across the SD Act and ASIO Act regimes, consideration be given to harmonising reporting obligations across both schemes.

118. As the Law Council has previously submitted in its 2012 submission to the PJCIS, the reporting requirements currently contained in the SD Act, could provide useful model.[9]

119. The SD Act contains a detailed reporting regime that includes the following features:

- anyone to whom a surveillance device is issued must provide a written report to an eligible Judge or eligible magistrate and to the Attorney-General[10] stating whether or not a surveillance device was used pursuant to the warrant. ;
- the Attorney-General is required to prepare, and table in Parliament, an annual report that also includes detailed information such as: [11] the number of applications for warrants and the number of warrants issued during that year;
- the chief officer of a law enforcement agency is required to keep a register of warrants and emergency authorisations, that includes information such as: [12] when warrants were issued; who they were issued by; who they were used by and any details of any variations or extensions of the warrant.

[9] The SD Act sections 48, 49.
[10] The SD Act section 44.
[11] The SD Act section 45.
[12] The SD Act section 47.

- the Ombudsman is required to inspect the records of each law enforcement agency (other than the ACC) to determine the extent of compliance with this Act by the agency and law enforcement officers of the agency[13] which must then be provided to the Attorney and tabled in Parliament. This report considers issues such as: were applications for warrants and authorisations properly made; were warrants and authorisations properly issued; were surveillance devices used lawfully; and were records properly kept and used by the agency.

120. The Law Council acknowledges that the ASIO Act already contains general provisions requiring the Director General to report to the Minister on the use of special powers, and that the IGIS has the power to conduct inquiries and request information about the use of these powers. However, incorporating more specific requirements into the ASIO Act relating to the use of surveillance devices would enhance accountability and oversight of the use of these covert, intrusive powers as well as further promoting consistency across the two existing regimes. The SD Act model could also be used to evaluate whether similar changes to reporting requirements should be made in relating to the issue and use of warrants under the TIA Act.

Access to third-party premises

121. Schedule 2 of the Bill also seeks to clarify that the search warrant, computer access, surveillance devices and identified person warrant provisions authorise access to third party premises to execute a warrant (sections 25, 25A and proposed section 26B of the ASIO Act – items 10, 19).

122. The amendments seek to implement PJCIS Recommendation 35 that the ASIO Act be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants.

123. The Law Council notes that while the amendments are limited to 'entering any premises for the purposes of gaining entry to or exiting the specified premises' they do not appear to acknowledge the exceptional nature and very limited circumstances in which the power should be exercised as also recommended by PJCIS Recommendation 35.

124. The Law Council understands that when executing a warrant, it may occasionally be necessary for an authorised person to enter third party premises other than the subject premises in order to enter or exit the subject premises. As noted in the Explanatory Memorandum, this may be because:

> *there is no other way to gain access to the subject premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common premises). It may also occur where, for operational reasons, entry through adjacent premises is more desirable (for example, where entry through a main entrance may involve a greater risk of detection). The need to access third party premises may also arise in emergency circumstances (for example, where a person enters the subject premises unexpectedly during a search and it is necessary to exit through third party*

[13] The SD Act section 48.

premises to avoid detection and conceal the fact that things have been done under a warrant).[14]

125. The Law Council considers that these amendments do not sufficiently consider the impact on the third party, including privacy implications as well as the potential for property damage to property.

126. If progressed the amendments should be modified to provide that entering a third party premises for the purposes of gaining entry to or exiting the specified premises when:

- there is no other way to gain access to the subject premises; or
- there is a substantial risk that that without access to the third-party premises the authorised officer would be detected.

127. The Law Council also suggests that consideration be given to the adoption of a singly privacy impact test during the warrant authorization process that would require the issuing authority to consider potential implications of the power to enter a third-party's premises for the privacy of the third-party. Alternatively, the ASIO Guideline 10 which requires proportionality and using as little intrusion into privacy as necessary could be strengthened if this amendment is enacted.

128. The Law Council encourages the PJCIS to seek clarification of measures which consider the potential for any damage to property.

Evidentiary certificates

129. Schedule 2 introduces new provisions that will enable evidentiary certificates to be issued under new section 34AA in relation to acts done by, on behalf of, or in relation to ASIO in connection with any matter in connection with a warrant issued under section 25A, 26, 27A, 27C or 29 or in accordance with subsection 26B(5) or (6), section 26C, 26D or 26E or subsection 27A(3A) or (3B) or 27F(5). These provisions relate to the use of special powers by ASIO, such as search warrants, computer search warrants, and listening and tracking device warrants. As the Statement of Compatibility accompanying the Bill provides:[15]

- certificates are to be prima facie evidence of the matters stated in the certificate (that is, certificates issued under the regime will be persuasive before a court, as distinct from a conclusive certificate that cannot be challenged by a court or a defendant);
- the regime is framed to ensure that an evidentiary certificate will only cover the manner in which the evidence was obtained and by whom but not the evidence itself. As such, the court will retain its ability to test the veracity of evidence put before it; and
- for operational security reasons, the proposed regime does not provide a conclusive list of the facts that the DG or a Deputy DG may include in an evidentiary certificate. The regime is not intended to provide a means for the prosecution to provide proof of any ultimate fact, or any fact so closely

[14] Explanatory Memorandum to the NSLA Bill, p 66.
[15] At paragraphs [45]-[47] of the Statement of Compatibility contained in the Explanatory Memorandum to the NSLA Bill.

connected certificate. The regime is not intended to provide a means for the prosecution to provide proof of any ultimate fact, or any fact so closely connected with an ultimate fact so as to be indistinguishable from it, or facts that go to the elements of the offence, without recourse for the course or the defendant to challenge the certificate and the facts it covers.

130. These amendments seek to implement PJCIS recommendation 37.

131. The Law Council acknowledges the need to ensure that certain sensitive operational capabilities are protected from disclosure in open court. It also supports efforts to ensure that Commonwealth legislation is consistent in this area.

132. When making this acknowledgement, the Law Council also recognises the fundamental importance of the principle of open justice and the need to protect and preserve the fair trial rights of individuals, which extend to the right to test evidence used against a defendant to a criminal charge. These principles demand that mechanisms designed to prevent disclosure of certain evidence must be considered exceptional, and limited only to those circumstances that can be shown to be necessary.

133. If the need for evidential certificates to protect the identity of ASIO officers and sources can be demonstrated, the regime must be developed in a way that seeks to balance the individual's right to a fair trial against the public interest in non-disclosure.

134. The Law Council is pleased that the proposed amendments follow the approach in the TIA Act and SD Act by making it clear that an evidentiary certificate only operates as *prima facie* evidence so that the trial judge may use his or her discretion under section 137 of the *Evidence Act 1995* (Cth) to exclude the evidence, which would apply where the probative value of a certificate is outweighed by the unfair prejudice it would cause to a defendant.

135. The types of matters listed in proposed new section 34AA (3) suggest that the certificates would include facts of a technical nature, however further consideration should be given to ensure that additional material that may address or prove the substantive elements of an offence is not incorporated.

136. This would help ensure that these certificates do not operate to preclude a defendant from being able to provide evidence inconsistent with the Crown's case in respect of information contained in a certificate.

<u>Further changes to ASIO warrant processes in schedule 2</u>

137. Schedule 2 makes a number of other changes to the existing warrant process in the ASIO Act.

138. These include amendments that will:

- enable the DG (or another person appointed by the DG) to authorise a class of persons to exercise powers under a warrant, not simply an individual. This will provide ASIO with flexibility to encompass a broad range of appropriate persons to exercise powers under a warrant or request information or documents from operators of aircraft or vessels;
- clarify that the use of reasonable and necessary force provided for in current paragraphs 25(7)(a), 25(5A)(a) and 27A(2)(a) of the ASIO Act may be used at

any time during the execution of a warrant, not just on entry, when it is authorised in the warrant. The use of force would extend to using reasonable and necessary force against a person in situations where a person tries to obstruct the execution of a search warrant, for example; and

- enable the Attorney-General to vary warrants. This is particularly important in situations where there is an administrative error or a change in circumstances. A warrant cannot be varied to extend the total period for which it is in force beyond 90 days for search warrants, and beyond a total period of six months for all other warrants issued by the Attorney-General under Division 2 of Part III. The DG's request must set out the relevant facts and grounds supporting the variation request.

139. Given the short time frame for this inquiry, the Law Council has not been able to undertake a detailed analysis of these changes, however on the basis of its past advocacy on similar proposed reforms it provides the following comments.

Amendments to authorise a class of persons to exercise warrant powers

140. These amendments would enable the DG (or another person appointed by the DG) to authorise a class of persons to exercise powers under a warrant. The Law Council recognises that this recommendation is designed to address practical inefficiencies faced by ASIO when seeking to execute warrants. It notes that flexibility already exists in terms of the execution of warrants by virtue of section 29 of the ASIO Act, which allows the DG to list a number of persons authorised to execute a warrant rather than specifying a particular officer. If the need for further flexibility can be demonstrated and this recommendation is pursued, the Law Council suggests that the views of the IGIS be sought so as to obtain a clear understanding of the impact of this change on their reporting and oversight functions. For example, information should be sought as to whether the absence of a requirement to list officers by name hinders any existing processes undertaken by IGIS when reviewing whether warrants have been issued and executed correctly.

Amendments relating to the use of force in the exercise of a warrant

141. The Law Council recognises that in certain circumstances it may be necessary to use reasonable force during the execution of a search warrant, for example, obtain access to a locked room/cabinet, or to use force to install or remove a surveillance device. However, any amendments to clarify that reasonable force can be used at any time for the purposes of executing the warrant should contain the existing safeguards which require that the use of force be reasonable and necessary to do what is required to execute the warrant.

142. For this reason, the Law Council supports the PJCIS's recommended safeguard of limiting an amendment for the use of force to be applied only to property and not persons. It is concerned by the proposals in this Bill that expressly authorise the use of force against a person in certain circumstances, noting that this contravenes the PJCIS recommendation. While it acknowledges that the use of this force must be authorised, and necessary and reasonable to do the things specified in the warrant, it nevertheless sets an expectation that the use of force by a person authorised – who may include people other than ASIO employees[16] – will sometimes be acceptable. In this context, the Law Council notes that in the existing ASIO Act, the only provisions which appear to expressly contemplate force being used against a person apply in

[16] See existing section 24(1) of the ASIO Act, as well as proposed new section 24(2).

the context of taking a person into custody and detaining them in relation to the special powers relating to terrorism offences under Division 3, Part III.[17]. Further, this use of force has specifically been specifically reserved for police officers, not ASIO officers. The Law Council considers that this more appropriately reflects the role of the police officer as a trained enforcer of the law.[18] It does not support those provisions which provide for the use of force to be used in respect of persons.

143. The Law Council also suggests that consideration be given to the adoption of a single privacy impact test (consistent with its past advocacy) during the warrant authorisation process that would require the issuing authority to consider the potential implications of the power to use force at any time during the execution of the warrant for the privacy and other rights of the occupants of the premises. Alternatively, the ASIO Guideline 10 which requires proportionality and using as little intrusion into privacy as necessary could be strengthened if this amendment is enacted.

Amendments enabling the Attorney-General to vary warrants

144. The Law Council supports moves to improve administrative efficiencies in the warrant process, including changes to processes that would enable administrative errors to be resolved in a timely way. However, it holds concerns with proposals that may operate to dilute existing safeguards designed to require the issuing authority to have regard to certain criteria before authorising the use of exception and intrusive powers. For this reason, the Law Council considers that ASIO officers should be required to seek a new warrant in every instance in which there is a significant change in circumstances – which could include a change in the premises subject to a search warrant (noting that a change in premises from a person's home to a large workplace could have broad privacy implications), the identity of a person subject to a listening device or tracking device, or the range of activities needed to be authorised to execute a warrant. Similarly, the Law Council considers it to be appropriate that ASIO seek a new warrant if an existing warrant has expired, even if the intelligence case remains unchanged. In both cases, there is a strong public interest in requiring ASIO to satisfy a rigorous authorisation procedure.

145. While the Explanatory Memorandum states that the power to vary warrants 'will only be used for variations of a relatively minor nature' and 'where there have been significant changes to the circumstances which applied when the original warrant was issued, a new warrant will be sought'[19] However, proposed 29A does not limit variations which can be made by the Minister to variations of a minor nature, other than specifying that there is a maximum period of extension. The Law Council recommends that proposed section 29A be amended to reflect that the power to vary a warrant only applies to amendments of a minor or technical nature.

Schedule 3 – Protection for Special Intelligence Operations

146. Schedule 3 amends Part III of the ASIO Act by inserting a new Division 4, which establishes a statutory framework for the conduct of SIOs by ASIO. New Division 4 seeks to implement Recommendation 28 of the PJCIS's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* of May 2013 (PJCIS Report). The PJCIS recommended that an SIO scheme be established, similar to the

[17] Section 34V of the ASIO Act.
[18] The police may also use reasonable and necessary force against a person in executing warrants – for example, under section 3G of the Crimes Act, which permits the use of such force in relation to an ordinary search warrant.
[19] Explanatory Memorandum to the NSLA Bill, p 92.

controlled operations regime in Part IAB of the *Crimes Act 1914* in relation to the covert activities of law enforcement agencies.

147. The Law Council understands that this SIO proposal is designed to ensure that appropriate protections are in place for ASIO officers and human sources who become involved in criminal activity during the course of an undercover operation. The proposed scheme would allow the DG or Deputy DG to grant a written SIO authority which would give ASIO employees and other human sources immunity from criminal and civil liability for specified conduct for a specified period.

148. The Law Council cautions against attempts to replicate – even in a modified form as contained in the NSLA Bill[20] – those powers currently available to law enforcement agencies, such as protection from liability under controlled operations, within the ASIO Act. These efforts risk ASIO employees and human sources engaging in unlawful activity on domestic soil against Australian citizens. It would threaten public confidence in the relationship between the citizen and the state by providing such persons with indemnity if they break the law. In this respect, it refers to a key tenet of the rule of law that no one should be regarded as above the law, and all people should be held to account for a breach of the law, regardless of rank or station.

149. The Law Council is not convinced of the necessity of an SIO scheme for ASIO to fulfil its statutory functions. ASIO officers are already permitted, for example, under the TIA Act and the ASIO Act to engage in conduct that would otherwise be considered unlawful (for example, intercepting communications and searching premises) and are not granted immunity from civil and criminal prosecution.

150. Under existing provisions, ASIO officers who become involved in criminal activity during the course of an undercover operation can also be protected from prosecution by the exercise of the CDPP's discretion not to prosecute. It would be highly unlikely that an ASIO officer would be prosecuted for the activities performed during a covert operation.

151. The Explanatory Memorandum notes, as part of its justification for the scheme, that ASIO employees or affiliates could be exposed to prosecution for preparatory terrorism offences in the course of their duties.[21] However, the Law Council considers an SIO would not be necessary in this context if these offences were properly defined. That is, if the terrorism offences were refined more narrowly, they would not capture the conduct of ASIO employees and affiliates.

152. The Law Council considers that relying on prosecutorial discretion to prosecute is appropriate, given the distinction between ASIO (an intelligence gathering agency with less identifiable operational need to engage in criminal activity) and the AFP.

153. This distinction is important. ASIO is not accountable through the criminal trial process in the way that a law enforcement agency is, and it is therefore not governed by the very strict chapter 3 of the Constitution jurisprudence that governs the behaviour of law enforcement agencies. It occupies a different constitutional, administrative and therefore policy position.

[20] The Law Council notes that while the SIO scheme is based broadly on the controlled operations scheme in the Crimes Act, modifications have been made. These modifications, as noted in the Explanatory Memorandum, are to reflect the differences between a law enforcement operation to investigate a serious criminal offence in order to gather admissible evidence, and a covert intelligence-gathering operation conducted for national security purposes.
[21] Explanatory Memorandum, p 15.

154. For example, as previously noted by the Law Council, because ASIO's statutory functions currently do not extend to gathering evidence in support of criminal prosecutions, it does not have the same obligations as those imposed on law enforcement agencies to inform prospective interviewees, particularly those under suspicion, about their rights to silence and to legal representation.[22]

155. However, the Law Council recognises that the above arguments have not been supported by either the PJCIS or the previous INSLM (who recommended that consideration be given to the introduction of a legislative scheme to provide ASIO and its human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations).[23]

156. If an authorised intelligence operations scheme is developed in accordance with the PJCIS's and INSLM's previous recommendations, the Law Council considers that it should include rigorous safeguards and accountability mechanisms in recognition of the particular role, functions and powers of ASIO.

157. In this regard, the Law Council emphasises that the PJCIS recommended a SIO scheme on the condition that it would be subject to similar safeguards and accountability arrangements as apply to law enforcement agencies under the controlled operations regime under the Crimes Act. The Law Council agrees that if such a scheme is to progress, it is critical that ASIO's actions should be regulated by comparable safeguards which are at least as strict as those under the controlled operations regime. It is concerned, however, that the proposed SIO scheme falls well short of the safeguards in the controlled operations regime in a number of important respects. It also considers that further safeguards are warranted in respect of the SIO regime.

158. The Law Council acknowledges and supports a number of safeguards contained in the NSLA Bill, including:

- a requirement that an authorisation for an SIO specify the nature of the special intelligence conduct a person may engage in, the persons authorised to perform such conduct;
- Proposed subsection 35C(1) provides that an authorising officer may grant an authority to conduct an SIO, if an application is made pursuant to section 35B and the authorising officer is satisfied, on reasonable grounds, of the matters set out in subsection 35C(2). These matters are:
  - the SIO will assist the organisation in the performance of one or more special intelligence functions, and the circumstances are such as to justify the conduct of an SIO: paragraphs 35C(2)(a) and (b);
  - any unlawful conduct involved in conducting the SIO will be limited to the maximum extent consistent with conducting an effective SIO: paragraph 35C(2)(c);
  - the SIO will not be conducted in such a way that a person is likely to be induced to commit an offence against a law of the Commonwealth, or a State or Territory, that the person would not otherwise have intended to commit: paragraph 35C(2)(d), and

[22] Law Council of Australia, Submission to the PJCIS Report, p 58.
[23] Recommendation VI/9, INSLM, *Independent National Security Legislation Monitor Fourth Annual Report* , 28 March 2014

- the conduct involved in an SIO will not cause death or serious injury to any person, or involve the commission of a sexual offence against any person, or result in significant loss of property or serious damage to property: paragraph 35C(2)(e).

- reporting requirements to the Attorney-General and to the IGIS. Proposed subsection 35Q(1) provides that the DG must give the Minister, and the IGIS, a written report in respect of each six-month period in which an SIO is in effect;

- reporting requirements to Ministers and the Parliament via ASIO's annual report.[24] Proposed subsection 94(2A) establishes reporting requirements in relation to ASIO exercise of powers under new Division 4 of Part III. Proposed subsection 94(1C) provides that ASIO's annual report must include a statement of the total number of applications made under section 35B for SIO authorities, and the total number of authorities granted under section 35C during the reporting period; and

- oversight by the IGIS and PJCIS.

159. However, the Law Council holds strong concerns about a number of features of the proposed SIO scheme, as discussed below.

Proposed definition of SIO

160. The definition of a controlled operation in the Crimes Act requires that it must be carried out for the purpose of obtaining evidence that may lead to the prosecution of a person for a 'serious Commonwealth offence'.[25] A serious Commonwealth offence means certain Commonwealth offences which are punishable on conviction by imprisonment for a period of 3 years or more.[26]

161. In contrast, the comparable proposed provisions defining a SIO are not so contained to more serious investigations. They refer to an operation 'that is carried out for a purpose relevant to the performance of one or more 'special intelligence functions'. Special intelligence functions include several of ASIO's core functions of obtaining intelligence relevant to security, communicating intelligence for security purposes, obtaining foreign intelligence and cooperating with other intelligence and law enforcement bodies.[27] This is a very broad definition which could potentially apply to most of ASIO's core operations. The Law Council considers that it could be mitigated through amendments to the threshold authority test (see further below).

162. A SIO may be authorised for an operation which 'may involve' an ASIO employee or an ASIO affiliate in special intelligence conduct.[28] This is a looser requirement than for a controlled operation, which must involve the participation of law enforcement officers[29], in order to meet the controlled operation definition. Given that the scheme

[24] See new section 35Q of the NSLA Bill. As mentioned in the note to proposed section 35Q, the IGIS has oversight powers in relation to conduct engaged in accordance with this Division: see section 8 of the IGIS Act. The IGIS may The IGIS may also exercise the information-gathering powers under the IGIS Act in respect of operations under Division 4. This includes the power to compel the production of documents or the provision of information, and the power to compel a person to give evidence under oath or affirmation. Item 4 inserts a
[25] Or a serious State offence with a federal aspect: subsection 15GD(1)(b) of the Crimes Act
[26] Section 15GE of the Crimes Act
[27] Section 4 of the NSLA Bill, which refers to paragraph 17(1)(a), (b), (e) or (f) of the ASIO Act
[28] Section 4 of the NSLA Bill
[29] Subsection 15GD(1) of the Crimes Act

(and its indemnities) can apply to 'persons authorised' (who apparently extend to persons other than ASIO employees and affiliates) and there is no requirement that core functions are conducted by ASIO employees, this is cause for concern. It means that technically, no ASIO employee need ultimately be part of the operation of the scheme. This raises concerns about the level of accountability involved.[30] The Law Council considers that if, contrary to its recommendations discussed below, civilian participants are to be included in the scheme, it would seem prudent to ensure that an ASIO employee must be involved in a SIO.

Test for authority

163. A controlled operations scheme must not be authorised unless an authorising officer is satisfied on reasonable grounds of a number of matters, including that:

- a serious Commonwealth offence[31] has been, is being, or is likely to be committed.[32] The comparable provision for SIOs is that the operation 'will assist ASIO in the performance of one or more special intelligence functions'.[33] The Law Council considers that this should be amended so that the SIO must 'substantially assist' ASIO in the performance of its functions.

- the nature and extent of the suspected criminal activity are such as to justify the conduct of a controlled operation.[34] The comparable provision for SIOs is that 'the circumstances are such as to justify the conduct of a SIO'.[35] This is a looser description. The Law Council considers that it should be amended so that 'the circumstances are sufficiently serious as to justify the conduct of a SIO'.

- the proposed controlled conduct will be capable of being accounted for in a way which will enable the reporting requirements contained in Division 4 of Part 1AB of the Crimes Act to be complied with.[36] There is no similar provision included, which heightens concerns that there will be a lack of accountability in relation to SIOs (see further concerns below). The Law Council queries why there is no such provision in the Bill.

164. That any conduct involved in the controlled operation will not (amongst other possibilities) seriously endanger the health or safety of any person.[37] While other requirements, such as that the conduct will not cause death or serious injury, are included in proposed section 35C (as in the Crimes Act), the Law Council queries why such a provision is not also included.

165. That any role assigned to a civilian participant in the operation is not one which could be adequately performed by a law enforcement officer.[38] A parallel provision is not included in relation to the proposed SIO scheme, which can permit immunity to 'persons authorised' (who do not appear to be limited to ASIO employees or affiliates). The Law Council considers that if, contrary to its recommendations

[30] See also later discussion about the lack of a person appointed with responsibility for the scheme's operation.
[31] Or serious State offence with a federal aspect.
[32] Section 15GA(2)(a)(i) of the Crimes Act.
[33] Proposed subsection 35C(2)(a) of the NSLA Bill.
[34] Section 15GA(2)(b) of the Crimes Act.
[35] Proposed subsection 35C(2)(b) of the NSLA Bill.
[36] Section 15GA(2)(a)(e) of the Crimes Act.
[37] Subsection 15GA(2)(g) of the Crimes Act.
[38] Subsection 15GA(2)(h) of the Crimes Act.

discussed below, civilian participants are to be included in the scheme, such a safeguard is necessary.

Immunities

166. There are also key differences in the immunities provided between the proposed SIO scheme and the controlled operations scheme, as follows.

- *Civil liability and compensation* - While the controlled operation scheme provides participants with criminal immunity if certain conditions are met,[39] it provides only that the Commonwealth must indemnify a participant in a controlled operation against any civil liability under section 15HB.[40] In addition, it provides that if a person suffers loss of or serious damage to property, or personal injury, in the course of, or as a direct result of a controlled operation, the Commonwealth is liable to pay that person compensation (section 15HF of the Crimes Act).[41] In contrast, proposed section 35K provides simply that a participant in a SIO is not subject to any civil liability provided that the criteria in the section are met. It does not provide for indemnification of the participant by the Commonwealth. Nor is there a proposed section, equivalent to section 15HF of the Crimes Act, which provides for the Commonwealth to pay compensation in respect of serious damage to property or personal injury.

  While the Explanatory Memorandum notes that ASIO is not precluded from paying compensation by proposed section 35K to an individual, the different wording of that section in comparison to section 15HB of the Crimes Act, combined with the omission of an equivalent section to 15HF, together appear to be designed to reduce the possibility that a person who was injured or suffered significant property damage[42] as a result of a SIO could successfully pursue a civil claim against the Commonwealth. This is exacerbated by the narrowly defined exception from the authorised disclosure offence for the provision of legal advice (see further below).

  The Explanatory Memorandum notes that the IGIS has the discretion to recommend that ASIO pay compensation to a person in appropriate cases. However, the Law Council is concerned that ASIO's liability for compensation for serious property damage or personal injury should not be left to the IGIS. In addition, it is concerned that the IGIS' oversight functions will be substantially impaired for the reasons set out further below.

  The Law Council considers that the wording of proposed section 35K should be amended to provide for indemnification from civil liability as under section 15HB of the Crimes Act. In addition, it considers that an equivalent to section 15HF providing for compensation to be payable should be included.

- *Immunity for conduct likely to cause death, serious injury* etc. - Under the controlled operations scheme, a person is not immune (or indemnified) from criminal or civil liability if his or her conduct fails to meet certain criteria

[39] Section 15HA of the Crimes Act.
[40] Section 15HB of the Crimes Act.
[41] Section 15HF of the Crimes Act.
[42] While unlike the controlled operations scheme, proposed section 35K specifically does not provide immunity to a participant if his or her conduct causes significant loss or, or serious damage to property, the Law Council queries how, in the circumstances, an individual who suffered such loss would be in a position to claim against that individual – a participant in a covert operation - directly.

including that he or she must not engage in any conduct that is likely to cause death, serious injury or the commission of a sexual offence against a person.[43] In contrast, the proposed section 35K provides for criminal and civil immunity provided that the conduct does not cause death or serious injury or involve the commission of a sexual offence.[44] This means that unlike the controlled operations scheme, a person can be immune from liability even if he or he engages in conduct which was likely to, but did not ultimately, cause death or serious injury or result in a sexual offence. The Law Council is concerned that without the equivalent safeguard to the controlled operations scheme, this may result in reckless behaviour.

- *Civilian participants* - Under the controlled operations scheme, a person is not immune from criminal or civil liability if he or she is a civilian participant in the operation and does not act in accordance with the instructions of a law enforcement officer. There is no such provision in proposed section 35K. This adds to the concerns already highlighted about the lack of accountability for the conduct of non-ASIO personnel in SIOs. The Law Council considers that if, contrary to its recommendations discussed below, civilian participants are to be included in the scheme, such a safeguard is essential.

- *Exceptions from immunity for certain conduct* - It is clear that under the controlled operations scheme that the provisions under the Crimes Act which protect participants from criminal and civil liability provided to participants do not apply in relation to a range of law enforcement conduct that is, or could have been, authorised by law. This includes the arrest or detention of individuals, searches of individuals or premises, searches or seizures of property, forensic procedure, electronic surveillance devices or telecommunications interception, identification procedures, the acquisition or use of assumed identities, or any other matter concerning powers of criminal investigation.[45] Therefore, if a law enforcement officer engages in such conduct, he or she will not be protected from liability if he or she does not meet the standards for that conduct which are prescribed in law.

  In contrast, proposed section 35L is less clear on this point. It provides that Division 4 of Schedule 3 (which governs SIOs) does not of itself allow ASIO to do an act without it being authorised by warrant under the ASIO Act or TIA Act. It also provides that ASIO must still obtain particular telecommunications data in accordance with the TIA Act (which requires authorisations to access the data).[46] Section 35L clarifies that a warrant must still be sought where required, and that certain information can only be obtained with the necessary authorisation. However, it is less clear whether an officer who falls short of the prescribed standards of the warrant or authorisation, or otherwise attracts civil or criminal liability for example in executing the warrant or obtaining the information, as part of a broader SIO, would be liable for that conduct. The Law Council recommends that the PJCIS seek clarification on this point. Proposed section 35L could, for example, be amended to provide that the immunities set out in proposed section 35K do not apply in respect of the acts contemplated in section 35L. Alternatively, proposed section 35D, which relates to the authority for the SIO, could be amended so as to require that

[43] Subsection 15HA(2)(d), subsection 15HB(d) of the Crimes Act.
[44] Subsection 35K(e) of theNSLA Bill.
[45] Section 15HC of the Crimes Act.
[46] Under Division 3 of Part 4-1 of the TIA Act.

under an SIO, persons authorised must comply with all conditions or requirements relating to warrants or the relevant TIA Act provisions.

Duration

167. A controlled operation certificate lasts only three months unless it is renewed in three month increments (up to a maximum of 24 months) by a nominated member of the Administrative Appeals Tribunal.[47]

168. In contrast, a SIO authority may operate for a maximum of 12 months.[48] It may be varied up to that maximum by the authorising officer (the DG or Deputy DG). The Law Council queries the rationale for the significantly longer timeframes which are proposed for SIOs versus controlled operations schemes. If the PCJIS accepts that there is a rationale for SIOs to operate for a longer period, the Law Council considers that the prescribed maximum duration should be not more than six months. It notes that containing the period of an SIO helps to ensure accountability by limiting the SIO to special intelligence conduct which is clearly foreseeable in the circumstances.

Variation

169. Variations under the controlled operations scheme can only be considered after consideration of a range of criteria which replicate the initial threshold test for the scheme's authorisation (which as discussed above, are more stringent than for proposed SIOs).[49] However, proposed subsection 35F(4) provides that the authorising officer must only: be satisfied on reasonable grounds that the operation will assist ASIO in the performance of its special intelligence functions, and consider it appropriate to do so. There is no requirement to reconsider the range of factors set out in proposed subsection 35C(2).

170. This is significant. It is proposed that a SIO may initially be authorised on the basis that the authorising officer is satisfied on reasonable grounds that unlawful conduct will be limited to the maximum extent possible, that it will not be conducted in a way in which a person is likely to be induced to commit an offence, and that any conduct will not cause death, serious injury or a sexual offence, or serious damage to property. However, its scope may later be expanded significantly under a process in which the – or another – authorising officer is not required to be satisfied on reasonable grounds of those matters.

171. The Law Council considers that SIOs should not be subject to variation – or at least significant variation – without an authorising officer being satisfied of the same criteria which were applicable during the initial authorising process.

Authority

172. The formal authority for a controlled operation must specify a range of important details, including the principal law enforcement officer who is responsible for the conduct of the controlled operation. In contrast, under proposed section 35D, the SIO authority must only identify the persons authorised to engage in special intelligence conduct. There is no ASIO official specified who has operational responsibility for the SIO.

[47] Crimes Act section 15GT. Where an 'urgent' application is made for a controlled operation, the authorisation will expire after 7 days and cannot be renewed: Crimes Act 15GU(5)(b)(ii).
[48] Proposed paragraphs 35D(1)(d) and 35F(f).
[49] Section 15GQ and 15GV of the Crimes Act.

173. Secondly, the controlled operation formal authority must specify the nature of the criminal activity in respect of which the controlled conduct is to be engaged in. It must also specify the nature of the controlled conduct that participants may engage in, in a manner which clearly differentiates the authorization of law enforcement participants' permissible conduct from civilians' permissible conduct (which is restricted to 'particular' conduct specified). As well, it must identify (to the extent known) the person or persons targeted. In contrast, proposed section 35D proposes merely that the SIO authority must provide 'a general description of the nature of the special intelligence conduct' that persons authorised may engage in.

174. The Law Council notes that the criminal and civil liability for participants which is set out in proposed section 35K will only apply if the participant 'engages in the conduct in accordance with the special intelligence authority to conduct the SIO'.[50] The Explanatory Memorandum emphasises that the immunity is 'limited to a person's conduct that is undertaken as part of an authorised SIO, which the person is authorised to undertake by the relevant SIO authority'. It is therefore critical that the authority is sufficiently specific in its guidance.

175. Further, the Law Council queries how, under the contents of the authority proposed in section 35D, it is expected that SIOs can function in a responsible, accountable manner – bearing in mind that such operations render participants with certain immunity from criminal or civil liability – when there is no responsible officer appointed, and an unacceptable lack of detail or guidance is required in the authority as to the nature and scope of the conduct to be authorised. It also queries how oversight or scrutiny by the IGIS is possible in practice without the inclusion of such details in the authority.

176. The Law Council recommends that proposed 35D be amended to: provide a specific description of the special intelligence that is sought as part of the SIO, a specific description of the special intelligence conduct that persons may engage in in a manner which distinguishes the role of civilian participants (if they are to be included in the scheme – see further discussion below) from ASIO employees or affiliates, specify (to the extent known) the persons, premises or objects to be targeted, and appoint an ASIO employee equivalent to principal law enforcement officer level as the responsible officer for the operation.

Reporting and oversight

177. The Law Council's concerns about the proposed SIO regime are heightened by the insufficient accountability, records, reporting and oversight mechanisms in relation to the scheme, compared to the controlled operations scheme. While it understands that proposed Division 4 would be subject to the IGIS' statutory powers of inquiry, it queries how such oversight will be meaningful in light of these concerns, as follows:

- The controlled operations scheme contains stringent reporting mechanisms. For example, the chief officer must submit a report to the Ombudsman every six months setting out a range of details about controlled operations, including the number of authorities granted or varied, the number of applications including variation applications, the number of applications refused.[51] It must also contain details for each controlled operations authority concerning the date of commencement and cessation, the outcomes of the controlled operation, the nature of the criminal activities against which the controlled

[50] Paragraph 35K(b) of the NSLA Bill.
[51] Section 15HM of the Crimes Act.

operations were directed, the identity of the person targeted, the nature of the controlled conduct engaged in, details of any serious damage to property or personal injuries occurring in the course of the operations, the number of authorities cancelled. The Ombudsman may also require additional information covering a controlled operation to which a report relates. The report must also be given to the Minister.

- In contrast, proposed section 35Q states only that the DG must give IGIS and the Minister a written report every six months. It is silent on what must be contained in that report save that it must report on the extent to which the special intelligence operation has assisted ASIO in the performance of one or more special intelligence functions. Such a reporting requirement is clearly inadequate.

- The controlled operations reporting scheme is supported by a requirement[52] that the chief officers provide annual reports to the Minister regarding controlled operations. This must contain key information including that required to be provided to the Ombudsman, including the nature of the criminal activity, outcomes of the controlled operation, nature of the controlled conduct and damage to person or property. This information must then be tabled (minus certain sensitive details) before Parliament. By contrast, proposed subsection 94(2) restricts similar reporting to the Minister (which is also to be laid before Parliament) to the total number of applications made during the year for the granting of special intelligence operation authorities, and the total number granted.

- There are also requirements under the Crimes Act that certain documents connected with controlled operations to be kept under section 15HP, including applications, authorities, variations and cancellations. No such requirement is included in proposed Division 4.

- Further, there are requirements that the Ombudsman regularly (at least every 12 months) inspect the records of each authorising agency to determine the extent of compliance with the provisions governing controlled operations by the agency and law enforcement officers. The Ombudsman must provide an annual report to the Minister in respect of this work (laid before Parliament minus certain sensitive information).[53] No such provisions are included which contain the equivalent requirements of the IGIS in relation to special intelligence operations.

178. As noted above, the Law Council recognises that the IGIS has general oversight functions, including the power to compel documents and evidence under oath. However, given the lack of specific detailed reporting and record keeping requirements under the proposed SIO scheme compared to the controlled operations scheme, combined with a lack of an onus on the IGIS to inspect and report on SIOs, it queries how the IGIS oversight can be relied upon as an assurance that SIOs will operate in a transparent and accountable manner.

179. The Law Council recommends that specific reporting, record keeping and inspection provisions be incorporated into the SIO scheme which mirrors the same stringent requirements which are contained in the controlled operations scheme.

[52] Section 15HN of the Crimes Act..
[53] Section 15HO of the Crimes Act.

Other safeguards

180. Further, the Law Council considers that the proposed SIO safeguards could be further strengthened by the following measures:

- Authorisation by an independent and external authority.

  The Law Council notes that the NSLA Bill provides that it would be the DG or Deputy DG of ASIO who would be empowered to authorise intelligence operation certificates which would provide protection from criminal and civil liability for specified conduct for a specified period (such as 12 months).

  The Law Council considers this authorisation process could be enhanced by removing the role of the DG and replacing this with an independent and external issuing officer, such as a Judge or AAT member, in addition to the proposed oversight by the IGIS. As the Law Council has previously submitted in the context of controlled operations for law enforcement officers,[54] this type of independent oversight is necessary to ensure that controlled operations are only authorised and conducted in strictly defined circumstances.

- Extension of immunity from criminal and civil liability to informants.

  The Law Council has previously opposed controlled operation regimes that seek to provide immunity from criminal and civil liability to third parties such as informants,[55] As discussed above, that this appears to be contemplated in the NSLA Bill by the reference to 'a participant' which is defined as 'a person who is authorised under Division 4 of Part III to engage in special intelligence conduct, for the purposes of the SIO' (as proposed to be inserted into section 4 of the ASIO Act) and the definition of an SIO which may involve an ASIO employee or ASIO affiliate. The Law Council has previously submitted that this extension of indemnity is a cause for concern, and demands particularly robust external, independent authorisation processes that currently do not exist for controlled operations in respect of law enforcement officers and do not appear to be contemplated under this proposal. The Law Council has also submitted that, if obtaining admissible evidence from informants requires empowering police to confer immunity on known criminals, then such evidence comes at too high a price and is unlikely to be in the interests of justice in the long-term.

- A requirement that the IGIS is notified when an SIO authority has been approved not simply that a report be produced in respect of each six-month period in which an SIO is in effect as currently contemplated by proposed section 35Q.

- A requirement for a mandatory independent review of the operation of the effectiveness and implications of the scheme five years after its commencement as contemplated by the Discussion Paper.[56]

- Provision of a sunset clause which would allow the SIO scheme to cease to operate at a certain point in time unless the Australian Government

[54] Law Council of Australia submission to the Senate Committee on Legal and Constitutional Affairs Inquiry into the provisions of the *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009* (Cth) (10 August 2009).
[55] Ibid.
[56] Attorney-General's Department Discussion Paper, *Equipping Australia against Emerging and Evolving Threats*, July 2012, p 47.

demonstrates its continued necessity and effectiveness. The Law Council considers such a sunset clause appropriate given the extraordinary nation of the SIO scheme and the potential to adversely impact on an individual's rights and freedoms.

Admission in evidence in judicial proceedings

181. Proposed section 35A provides statutory guidance in the exercise of this discretion in relation to intelligence obtained as part of an SIO that is required to be used as evidence. The section seeks to ensure that such evidence is not excluded automatically through the general discretion of courts to exclude evidence that was obtained through unlawful conduct. Section 35A provides that such evidence is able to be adduced if it is otherwise admissible in accordance with general rules of evidence. For example, evidence gathered via an SIO might be excluded on the basis that its probative value is outweighed by its prejudice to the interests of a party.

182. Subsection 35A(1) preserves general judicial discretion in relation to the admission or exclusion of evidence, or to stay criminal proceedings, subject to the following two modifications:

- proposed subsection 35A(2) provides that a court may not exclude evidence solely because it was obtained as a result of a person's engagement in a criminal activity, if the person was a participant in an SIO, and the relevant conduct was within the scope of the SIO authority. Subsection 35A(2) applies exclusively to evidence obtained as a result of conduct that is authorised under an SIO. It does not extend to evidence obtained as a result of conduct which exceeds the scope of authority under an SIO authority, or conduct which pre-dated the grant of the authority; and

- an authorising officer may, under proposed section 35R, issue an evidentiary certificate in respect of any factual matters relevant to the granting of an SIO. Such a certificate is taken as prima facie evidence of the matters stated in the certificate. The evidentiary certificate creates a rebuttable presumption as to the existence of the factual basis on which the criteria for issuing a SIO were satisfied.

183. The proposed SIO scheme will grant ASIO employees and ASIO affiliates to engage in otherwise unlawful conduct.

184. The Law Council recommends that the PJCIS request further information about why this scheme is needed and how it will interact with the existing rules of evidence.

185. The Law Council, for example, would be concerned at any approach that would see these certificates used to establish prima facie evidence of the elements of any criminal offence. It further recommends that if evidentiary certificates are to be issued under section 35R, a safeguard be included in that section to ensure that the information contained in the evidentiary certificate is of a technical nature only and does not address the substantive elements of an offence.

New offences: unauthorised disclosure of information relating to a SIO

186. Section 35P will create two new offences relating to the unauthorised disclosure of information relating to a SIO by any person, including participants in an SIO, other persons to whom information about an SIO has been communicated in an official capacity, and persons who are the recipients of an unauthorised disclosure of information, should they engage in any subsequent disclosure.

187. The measure is designed to create a deterrent to unauthorised disclosures, which may place at risk the safety of another person or the effective conduct of an SIO.

188. Under subsection 35P(1) a person commits an offence if the:

- person discloses information; and
- information relates to a SIO.
- offence carries a penalty of five years imprisonment.

189. Paragraph 35P(1)(a) relates to the physical element of a person's conduct in disclosing information. As such, by reason of subsection 5.6(1) of the Criminal Code the fault element of intention applies.

190. Paragraph 35P(1)(b) relates to the physical element that the information must relate to a SIO. As such, by reason of subsection 5.6(2) of the Criminal Code the fault element of recklessness applies. A person may therefore be guilty if they intend to disclose information and he or she is aware of a substantial risk that the information relates to an SIO or will relate to an SIO, and having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

191. Proposed subsection 35P(2) creates an aggravated form of the offence in subsection 35P(1). The relevant aggravating elements, which are set out in paragraph (c), are that:

- the person intended, in making the disclosure, to endanger the health or safety of any person, or prejudice the effective conduct of an SIO, or
- the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of an SIO.

192. The fault element applying to the physical element in subparagraph 35P(2)(c)(i) is that of intention, pursuant to the express statement in the provision. The fault element applying to the physical element in subparagraph 35P(2)(c)(ii) is that of recklessness, by reason of subsection 5.6(2) of the Criminal Code. The aggravated offence is subject to a maximum penalty of 10 years' imprisonment.

193. The Law Council understands the importance of protecting participants in covert intelligence operations and the safety of participants or the effective conduct of such operations.

194. However, the Law Council considers that there are difficulties with the creation of these offences which must be addressed prior to possible enactment (discussed further below).

Current secrecy provisions

195. The Law Council queries the necessity of the proposed offences in light of the offences available under the current law.

196. In particular, the Law Council would like to draw the Committee's attention to the following which may already capture unauthorised disclosure of information relating to

an SIO: terrorism offences;[57] intentionally or recklessly causing harm to Australians overseas;[58] treason offences;[59] espionage offences;[60] secrecy offences in the Crimes Act;[61] and secrecy offences for employees of IS Act organisations.[62]

197. Given the timeframe for the current inquiry, the Law Council has not had the opportunity to review the extent to which these offences already cover the conduct proposed to be captured by the new offences in section 35P – or for that matter the increase in penalties for unauthorised disclosures by an ASIO employee or ASIO affiliate and the proposed unauthorised dealings offence (discussed further below). However, the Law Council considers that the PJCIS should inquire into the inadequacy of the current provisions in determining whether there is a legislative gap in the framework for the protection of information which the new offences in section 35P seek to address (or for which the NSLA Bill seeks to increase penalties or create an offence for unauthorised). If there is considerable overlap, the Law Council considers that the necessity of the new offences and increased penalties has not been demonstrated.

198. Further, the Law Council is of the view that this issue is particularly pertinent given the limited protection for whistle-blowers (discussed below).

Protection for whistle-blowers, lawyers etc.

199. The new offences in section 35P would potentially apply to a wide range of people from, for example, whistle-blowers, journalists, or lawyers seeking to disclose information about suspected wrongdoing relating to illegal conduct, corruption, maladministration etc.

200. The Law Council is concerned that the provisions will interfere with freedom of speech and prevent public discussion of important issues of public interest. The Law Council notes that there does not appear to be provision for a public interest disclosure scheme in the NSLA Bill.

201. In this regard, the Law Council notes that under the equivalent unauthorised disclosure offences which apply in relation to the controlled operations scheme, specific exceptions are included where: the person discloses the information to the Ombudsman or the Integrity Commissioner; and informs the person to whom the disclosure is made of his or her identity before making the disclosure; the information concerns a corruption issue or misconduct in relation to a controlled operation; the discloser considers that the information may assist the Ombudsman or Integrity Commissioner to perform their duties; and the discloser makes the disclosure in good

[57] Including: Division 101 of the Criminal Code – particularly given the definition of terrorism in section 100.1 of the Criminal Code and offences for example for committing a terrorist act and the pre-emptive offences which apply to the early stages of preparing for a terrorist act, including possessing things connected with terrorist acts (section 101.4), collecting or making documents likely to facilitate terrorist acts (section 101.5) and doing any other act in preparation of a terrorist act (section 101.6); and Division 102 of the Criminal Code which makes it an offence to intentionally provide support or resources to a terrorist organisation.
[58] Division 115 of the Criminal Code.
[59] Division 80 of the Criminal Code.
[60] Section 91.1 of the Criminal Code.
[61] Including: section 70 of the Crimes Act makes it an offence for current or former Commonwealth officers to disclose any facts they have learned or documents they have obtained by virtue of being a Commonwealth officer and which it is their duty not to disclose; and section 79 of the Crimes Act which sets out multiple offences where a person communicates official secrets.
[62] Sections 39, 39A and 40 of the IS Act which provide for specific secrecy offences to employees of IS Act agencies who release information obtained in the course of their employment.

faith.[63] There is no such exception in the proposed special intelligence operations scheme (which would be provided in relation to the IGIS, rather than the Ombudsman or Integrity Commissioner). This lack of a whistleblower exception is of real concern to the Law Council. It considers that at a minimum, such an exception must be included.

202. In addition, the Law Council recommends that the ASIO Act be amended to allow a person to seek legal advice in relation to the potential disclosure of the information. Such advice is essential in a person ascertaining his or her legal rights and obligations. Currently, an exception is included where the disclosure was for the purposes of any legal proceedings, as is the case under the relevant controlled operations scheme offences. However, under the controlled operations scheme, an exception is also provided for legal advice in relation to the controlled operation.[64]

203. The Law Council notes that these measures are subject to the public interest disclosure scheme contained in the *Public Interest Disclosure Act 2013* (Cth). However, this scheme only permits disclosure by a current or former 'public official' of information that tends to show, or that the public official reasonably believes tends to show 'disclosable conduct'.[65] Disclosable conduct may include conduct engaged in by an agency, public official or contracted service provider that relates to illegal conduct, corruption, maladministration, abuse of public trust, deception relating to scientific research, wastage of public money, or unreasonable danger to health and safety or to the environment.[66]

204. Therefore, the scheme would not apply to protect a journalist or a lawyer who receives information from a public official relating to an SIO and makes a subsequent disclosure in the public interest.

205. Further public interest disclosures by a public official to third parties, such as lawyers or journalists, must not consist of, or include, intelligence information or relate to the conduct of an intelligence agency. Emergency disclosures and disclosures to a legal practitioner must not consist of, or include, intelligence information.[67]

206. The Law Council understands the Public Interest Disclosure Act only applies to allow disclosure of information by an AIC employee in three very limited scenarios, namely:

- a public official would be protected for disclosing intelligence information to his or her immediate supervisor, an authorised internal recipient, or the IGIS but only where this relates to unlawful activity;[68]

- a public official would be protected for disclosing information relating to intelligence agencies (but not intelligence information) where there is a substantial and imminent danger to health, safety or the environment;[69]

[63] Subsections 15HK(3) and15HL(3) of the Crimes Act.
[64] Paragraphs 15HK(2)(c) and 15 HL(2)(c) of the Crimes Act.
[65] A public official includes public servants and parliamentary service employees, service providers under a Commonwealth contract, statutory office holders, staff of Commonwealth companies etc – see section 69 of the *Public Interest Disclosure Act 2013* (Cth).
[66] Section 29 of the *Public Interest Disclosure Act 2013* (Cth).
[67] Section 41 of the *Public Interest Disclosure Act 2013* (Cth) provides a comprehensive definition of 'intelligence information'.
[68] Subsection 26(1) of the *Public Interest Disclosure Act 2013* (Cth).
[69] Ibid.

- a public official would be protected for disclosing information relating to intelligence agencies to an Australian legal practitioner.[70] The legal practitioner, however, would need to hold an appropriate security clearance, and the protection would not extend to intelligence information such as operations, sources and methods.[71]

207. These circumstances appear more limited than the broader exceptions in the Crimes Act which allow a person to disclose information for the purposes of obtaining legal advice in relation to the controlled operation.[72]

- The Law Council queries how the average public official would find a legal practitioner with a security clearance, and also how practically they would seek advice about something that had happened during an SIO – which may, for example, have involved corrupt conduct or abuse of power, or injury to themselves or another person - without disclosing 'intelligence information'.

- Further, the Law Council is concerned that without such a provision in the SIO scheme other individuals who are not current or former public officials , such as journalists, or people who have been affected by the scheme – for example, because they have been injured or have sustained serious property damage – are likely to be in an invidious position. They may be prevented from obtaining, and their legal practitioners from providing legal advice, about their standing, if no legal proceedings are on foot.

208. While in order to satisfy the section 35P offences, the individual, employee or legal practitioner would need to know or be aware of a substantial risk that the information relates to an SIO, it is highly likely that they would decide that it would be unjustifiable to take any risk of seeking or providing legal advice in relation to ASIO conduct under the provisions as currently worded.

209. The Law Council notes that the offence would not apply through subsection 18(9) of the *Inspector-General of Intelligence and Security Act 1986* (Cth) (IGIS Act) if a document was dealt with for the purpose of producing information under subsection 18(1) of the IGIS Act. However, again this is a very limited protection for whistle-blowers and appears to only apply in relation to information that is formally requested by the IGIS under subsection 18(1) rather than volunteered by the person.

The unauthorised disclosure offences should not be based on a secretly declared SIO

210. SIOs are determined by the DG and because of their covert nature will generally not be known to the public. Accordingly, there are likely to be difficulties in proving that a person was aware of a substantial risk that the information related to an SIO or will relate to an SIO.

[70] Ibid.
[71] Ibid. See also Keiran Hardy and George Williams. 'Terrorist, Traitor, or Whistelblower? Offences and protections in Australia for Disclosing National Security Information.' Forthcoming in the University of New South Wales Journal, 2014. The Law Council has previously considered in detail security clearances for lawyers and has raised concerns with such an approach. See for example the Law Council's Anti-Terrorism Reform Project, October 2013, pp. 108-109 available at http://www.lawcouncil.asn.au/lawcouncil/index.php/divisions/criminal-law-and-human-rights/anti-terror-law?layout=edit&id=144.
[72] Paragraphs 15HK(2)(c) and 15 HL(2)(c) of the Crimes Act.

211. The Law Council is concerned that the practical effect of these measures will therefore result in severe intrusions on the freedom of speech as a person is unlikely to disclose a wide range of information for fear that it might relate to an SIO.

212. Further, there appears to be no requirement that the disclosure of the information relating to an SIO will or is likely to cause harm to another person or jeopardise the effective conduct of an SIO.

213. This situation is compounded by the fact that at trial, details of the SIO would not necessarily be revealed leaving a person in the position of not being able to in a trial know what the SIO related to in order to properly defend his or her case.

214. The Law Council's preliminary views are that legislation must therefore be further refined to avoid this situation. The offence contained in subsection 35P(1) should be removed from the Bill.

215. While the aggravated offence in subsection 35P(2) establishes a necessary nexus between the disclosure of the information relating to an SIO causing harm to the health or safety of another person or prejudicing the effective conduct of an SIO, it nonetheless still contains the defect that a person may not know or be aware that there is a substantial risk that the information relates to an SIO.

216. If Parliament determines that it is necessary to provide for an offence of unauthorised disclosure of sensitive information to protect the health or safety of any person or to prevent prejudicing the effective conduct of an SIO with the penalty of 10 years imprisonment, the offence provisions should not be based on potentially secretly declared SIOs by ASIO.

217. In addition, the Law Council suggests that the PJCIS seek further information regarding why the Part IAB Crimes Act framework for controlled operations, which includes a similar prohibition on disclosing information about controlled operations, contains a two-year jail term,[73] not five years as is proposed under the ASIO SIO regime. That is, the Law Council suggests the PJCIS inquire into why the ASIO SIO regime contains such a severe penalty when contrasted to the AFP controlled operations scheme.

Schedule 4 – Co-operation and information sharing

218. Schedule 4 amends the (ASIO Act to enable breaches of section 92 of the ASIO Act, which contains offences relevant to the non-disclosure of identity obligations, to be referred to law enforcement agencies for investigation. This amendment implements the Government's response to Recommendation 34 of the PJCIS's *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.

219. The Schedule also clarifies ASIO's ability to co-operate with the private sector both in Australia and overseas and implements the Government's response to Recommendation 33 of the Report of the PJCIS.

220. These measures are discussed further below.

[73] Subsection 15HK(1) of the Crimes Act.

Breaches of section 92 of the ASIO Act

221. Section 92 of the ASIO Act makes it an offence for a person to publish the identity of an ASIO officer. The offence is punishable by 12 months imprisonment.

222. However, section 18 of the ASIO Act limits the circumstances in which a person can communicate information or intelligence acquired through their association with ASIO. Information may only be passed to law enforcement agencies in relation to a 'serious crime' (defined as an offence punishable by imprisonment *exceeding* 12 months).

223. ASIO is currently precluded from passing information therefore about the possible commission of a section 92 offence to law enforcement agencies which carries a penalty not in excess of 12 months imprisonment.

224. The NSLA Bill seeks to amend section 92 to make it an offence to publish the identity of a current or former ASIO employee or ASIO affiliate, without the written consent of the Minister or DG.

225. Item 3 of Schedule 4 of the NSLA Bill inserts a new subparagraph 18(3)(b)(ia) to provide that the DG or a person authorised by the DG may communicate information to law enforcement if 'the information relates, or appears to relate, to the commission, or intended commission, of an offence against section 92 (publication of identity of ASIO employee or affiliate).

226. The communication of any breach of section 92 would only be made by the DG or a person acting within the limits of authority conferred on the person by the DG (in accordant with subsection 18(1) of the ASIO Act).

227. The Law Council understands the importance of keeping the identity of ASIO employees secret. The publication of a name or identifying information may place an officer and his or her family in personal danger, compromise ongoing ASIO activities, identify ASIO's operational practices and ASIO's ability to further use that officer may be compromised. In this sense, section 92 protects the privacy and security of ASIO officers and their families. Accordingly, the Law Council does not oppose ASIO having the ability to refer breaches of section 92 to law enforcement for investigation.

228. However, the Law Council notes that there may be times when it would be in the public interest to identify ASIO officers, for example, those who are likely to be involved in maladministration or in criminal acts.

229. The Law Council notes in this regard that it appears that the Bill does not exclude the possibility of a person in such a situation making a complaint to the IGIS. The Law Council encourages the PJCIS to seek confirmation of this important oversight mechanism.

230. The Law Council notes that in limited circumstances a disclosure of certain conduct may be permitted under the *Public Interest Disclosure Act 2013* (Cth) (so long as it does not relate to an intelligence operation or the identity of an ASIO employee).

231. In addition, the Law Council recommends that provision be made in the ASIO Act for a person to be permitted to seek legal advice in relation to the potential disclosure of the information. Such advice is essential in a person ascertaining his or her legal rights and obligations.

232. The Law Council notes that there is a need for the Government to clarify what types of information can be shared with the private sector and what legislative provisions governing the handling and dissemination of such information apply.

233. The Law Council regrets that in the time frame for this inquiry it has not had the opportunity to consider in detail the safeguards that apply on private sector co-operation contained in the ASIO Act. It therefore encourages the PJCIS to inquire into what safeguards apply and, in particular, to consider the risks that might be involved in disclosure of information to the private sector and whether bodies within this sector can be held to account for the handling and dissemination of such information.

Schedule 5 – Activities and functions of Intelligence Services Act 2001 agencies

234. Schedule 5 of the Bill seeks to:

- amend the IS Act (which applies to Australia's foreign intelligence agencies) to enable ASIS to undertake a new function, without a Ministerial authorisation, of co-operating with ASIO in relation to the production of intelligence on an Australian person or persons overseas in accordance with ASIO's requirements;
- create a new ground of Ministerial authorisation enabling the Minister responsible for ASIS to authorise the production of intelligence on an Australian person who is, or is likely to be, involved in activities that pose a risk to, or are likely to pose a risk to, the operational security of ASIS; and
- extend the protection available to a person who does an act preparatory to, in support of, or otherwise directly connected with, an overseas activity of an IS Act agency to an act done outside Australia.

235. The Law Council outlines below some general comments on the suitability of the current division of functions among AIC agencies prior to considering the measures contained in Schedule 5 the NSLA Bill.

Cooperation among AIC agencies

236. Australia has five agencies focused on foreign intelligence. There are three collection of intelligence agencies (ASIS, ASD and DIGO) and two with an intelligence assessment role (the Office of National Assessments – ONA – and the Defence Intelligence Organisation – DIO). Australia's intelligence agency, ASIO, incorporates both collection and assessment, and undertakes policy formulation and advice.[74] ASIO undertakes security intelligence to protect Australia's security interests within or outside of Australia.

237. The Law Council understands that generally the IS Act agencies engage in activities dealing with foreign threats to Australia's interests, while ASIO largely deals with Australia's response to domestic threats. Such a division was based on a traditional cold-war era division of work.

[74] Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, 20 July 2004, p 7 at http://www.dpmc.gov.au/publications/intelligence_inquiry/.

238. However, ASIO may collect foreign intelligence in Australia at the request of the Minister for Foreign Affairs or the Minister for Defence (sections 27A and B of the ASIO Act). That is, a key function of ASIO includes to obtain within Australia foreign intelligence pursuant to section 27A or 27B of the ASIO Act or section 11A, 11B or 11C of the TIA Act , and to communicate any such intelligence in accordance with the ASIO Act or the TIA Act (paragraph 17(1)(e) of the ASIO Act).

239. Similarly, as noted in the independent review of Philip Flood's *Report of the Inquiry into Australian Intelligence Agencies* (2004) (the Flood Report), ASIS's operational activities are not solely undertaken overseas. Collection of foreign intelligence in Australia, often in cooperation with ASIO, is a key part of its mandate.

240. The Law Council acknowledges that the terrorism threat since 11 September 2001 highlighted the need for an agency to be looking for a foreign threat (from foreign infiltrators) to domestic targets.

241. In this respect, the Law Council recognises the need for timely and effective cooperation between intelligence gathering agencies, which is particularly important to counter emerging threats to national security such as the collection of intelligence in respect of assessment of Australians fighting in Syria or for ISIS. There is no doubt that such threats demands cooperation between ASIO (with domestic capability) and ASIS (with international capability).

242. However, great care must be taken when seeking to amend the authorisation processes for the use of intrusive intelligence gathering powers.

243. Each Australian intelligence agency has its own clear statutory functions, its own oversight and reporting mechanisms and its own authorisation and warrant processes – all designed to recognise the exceptional nature of these agencies and to provide the parliament and the public with confidence that these agencies are operating within the law.

Permitting ASIS to cooperate with ASIO and produce intelligence on an Australian person

244. ASIO collects intelligence relevant to 'security' as defined in section 4 of the ASIO Act.[75] ASIS collects intelligence about the capabilities, intentions or activities of people or organisations outside Australia.[76] The current mechanisms which enable ASIO and ASIS to produce intelligence on Australian persons differ substantially.

245. Within the limits of the ASIO Act (which applies to Australia's external territories), ASIO can collect intelligence about an Australian of security interest who is overseas based on internal approvals whereas ASIS requires the approval of the Minister for Foreign Affairs and the agreement of the Attorney-General to do the same thing.[77]

246. The Law Council recognises that this produces an anomaly where the level of protection of the rights and interests of Australians who may be subject to surveillance or other intelligence gathering activities (including the rights of innocent third parties) may depend on which agency is collecting the intelligence. This

[75] See paragraph 17(1)(a) of the ASIO Act.
[76] Paragraphs 6(1)(a) and (b) of the IS Act.
[77] See subparagraph 8(1)(a)(i) and paragraph 9(1A)(b) of the ISA. Note that in any case if the activity was in Australia and required a warrant it could not be undertaken by either agency in the absence of a warrant. This includes, for example, if ASIO was to obtain intelligence about an Australian who is overseas by intercepting the calls made by that person to another person in Australia via the Australian telecommunications network. See also paragraph 17(1)(e) of the ASIO Act.

presents a need to consider how to most appropriately promote consistency across existing regimes, in a manner that builds upon the most rigorous existing authorisation processes associated with the use of intrusive intelligence gathering powers.

247. Proposed new section 13B of the IS Act seeks to allow ASIS, subject to the new section 13D, to undertake an activity or a series of activities for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person or a class of Australian persons where the DG or a senior ASIO position holder authorised by the DG, has notified ASIS in writing that it requires the production of intelligence on the Australian person or class of Australian person.

248. Division 3 will only apply to ASIS activities outside Australia and only when ASIS is undertaking activities to support ASIO in the performance of ASIO's functions.

249. A notice issued by ASIO under this provision notifies ASIS of a requirement to produce intelligence on an Australian person, or a class of Australian person. The notice may identify a number of Australian persons. This notice may not be required in certain circumstances although notification must be given to the IGIS.[78]

250. This measure is designed to implement the PJCIS's Recommendation 39 that where ASIO and an IS Act agency are engaged in a cooperative intelligence operation a common standard based on the standards prescribed in the ASIO Act should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person. This was followed by a recommendation by the previous INSLM that the IS Act be amended to facilitate intelligence collection and production by ASIS, ASD and DIGO without ministerial authorisation where the intelligence collection and production is at the request of the DG of ASIO and is for the purpose of assisting ASIO in the performance of its counter-terrorism function.[79]

251. The Law Council is pleased that there are a number of safeguards included in this proposal, including:

- proposed section 13D makes it clear that where ASIO is required to obtain a warrant under Division 2 of Part III of the ASIO Act of under Part 2-2 of the TIA Act, proposed section 13B does not allow ASIS to undertake the act. The effect of this section is that ASIS will still be required to obtain a Ministerial authorisation under section 9 of the IS Act before undertaking particularly intrusive activities overseas (for example, the use of tracking devices, listening devices and the interception of telecommunications);

- in undertaking an activity under this new Division, the limitations in subsection 6(4) and sections 11, 12 and 13 of the IS Act that apply to ASIS's functions will continue to apply;

- the notice may specify certain conditions that apply;[80]

- only certain authorised officers of ASIS will be able to produce intelligence on an Australian person in accordance with section 13B;[81]

[78] Subsections 13B(3) and(4) of the NSLA Bill.
[79] Recommendation VI/10, INSLM, *Independent National Security Legislation Monitor Fourth Annual Report*, 28 March 2014
[80] Subsection 13B(2) of the NSLA Bill.
[81] Subsection 13B(7) of the NSLA Bill.

- the Director-General of ASIS is to be satisfied of certain matters – including that there are satisfactory arrangements in place to ensure that activities will be undertaken under section 13B only for the specific purpose of supporting ASIO in the performance of its functions and there are satisfactory arrangements in place to ensure that the nature and consequences of acts done under section 13B will be reasonable, having regard to the purposes for which they are carried out;[82]

- the privacy rules made under section 15 of the IS Act will also apply to the communication of any intelligence information that concerns an Australian person;[83]

- if ASIO issues a notice under paragraph 13B(1)(d), the Director-General of ASIS must ensure that a copy of the notice is kept by ASIS and is available for inspection on request by the IGIS;[84]

- reporting requirements – proposed subsection 13F(4) provides that, as soon as practicable after each year ending on 30 June, the Director General of ASIS must give to the responsible Minister in relation to ASIS a written report in respect of activities undertaken by ASIS under section 13B during the year; and

- Ministerial Guidelines – section 13G into the IS Act to enable the responsible Minister in relation to ASIO and the responsible Minister in relation to ASIS to jointly make written guidelines relating to the undertaking of activities under section 13B.

252. The Law Council notes however that these safeguards could be strengthened by the NSLA Bill specifying what types of 'activities' could be approved, how long the approval would be for, and on what basis it could be approved or renewed. It notes that this proposal constitutes a significant departure from the current situation, under which Ministerial authorisation is required before ASIS can collect intelligence on an Australian person.

<u>ASIS' collection of intelligence on persons involved in activities in relation to its operational security</u>

253. Item 6 of Schedule 4 of the NSLA Bill implements the Government's response to Recommendation 38 of the PJCIS Report by inserting a new Ministerial authorisation ground. This new Ministerial authorisation ground will amend paragraph 9(1A)(a) to enable an IS Act agency to produce intelligence on an Australian person whose activities pose a risk, or are likely to pose a risk, to the operational security of ASIS.

254. It should be read in conjunction with the proposed definition of 'operational security' which means the protection of the integrity of ASIS operations from interference by a foreign person or entity or reliance on inaccurate information.[85]

255. The Law Council encourages the PJCIS to request further detailed information in relation to this proposal as it is not clear from the Explanatory Memorandum or past submissions to the PJCIS as to why a risk to the operational security of ASIS is not

[82] Section 13E of the NSLA Bill.
[83] Subsection 13F(2) of the NSLA Bill.
[84] Subsection 13F(3) of the NSLA Bill.
[85] Item 1 of the NSLA Bill which seeks to inserts such a definition into section 3 of the IS Act.

already covered by subsection 9(1A) of the IS Act. That is, the Law Council queries whether the scope of existing subparagraph 9(1A)(a)(iii), namely, the category of 'activities that are, or are likely to be, a threat to security' is already sufficiently broad to cover activities pose a risk, or are likely to pose a risk, to the operational security of ASIS.

256. The Law Council understands that the measure is designed to better protect the integrity of ASIS operations and its staff members and agents from the risk of being interfered with or undermined by foreign persons or entities (for example, non-State adversaries such as terrorist organisations) or where ASIS is at risk of relying on inaccurate or false information.[86]

257. The Explanatory Memorandum also provides that this ground is intended to address activities that pose a risk, or are likely to pose a risk, to the operational security of ASIS but are not, or are not likely to be, a threat to 'security' (for example, espionage or sabotage or interference by foreign governments) as defined in the ASIO Act.[87]

258. However, the Explanatory Memorandum does not provide examples of where an activity may pose a risk to the operational security of ASIS but will not be a threat to security. The Law Council suggests that the PJCIS seek such examples in order to determine the necessity of the proposed amendment.

259. The Law Council is also concerned that the establishment of this new ground involves a significant expansion the powers of IS Act agencies and will allow such agencies to produce intelligence on a greater number of Australian persons.

260. In this regard, the Law Council notes that while the intelligence produced must be relevant to the operational security of ASIS, ASD and DIGO may also seek a Ministerial authorisation from the Defence Minister to produce intelligence to assist ASIS.

261. Accordingly, if such an amendment is to be pursued the Law Council considers that such agencies be required to undertake a single privacy impact test (as discussed above).[88]

Schedule 6 – Protection of information from 'insider threats'

262. The Bill goes beyond implementing the PJCIS's recommendations and contains a number of measures designed at protecting the information of Australia's intelligence agencies from disclosure by persons who have accessed certain information while acting in a specified official capacity (for example, as an employee of the relevant agency) for ASIO or an IS agency.

263. The Explanatory Memorandum notes that the amendments will ensure that the secrecy offences in the ASIO Act and the IS Act 'target, denounce and punish

[86] As noted in the Explanatory Memorandum to the NSLA Bill, p 120.
[87] Ibid.
[88] The Law Council notes that the existing safeguards in the IS Act would apply to this new Ministerial authorisation ground. This includes the requirements for all authorisations to be made available for inspection by the IGIS. Before issuing an authorisation under this new ground, the Minister responsible for the IS Act must be satisfied of the factors in subsection 9(1). In accordance with paragraph 9(1A)(b), where the Australian person is also, or is also likely to be, involved in an activity or activities that are, or likely to be a threat to security, the Minister responsible for the IS Act will still be required to obtain the agreement of the Attorney-General before issuing an authorisation.

appropriately the wrongdoing inherent in the intentional unauthorised communication of, or dealing with, the official records or information of AIC agencies'.[89]

264. These measures are discussed below.

Increase in penalty for unauthorised disclosure of information

265. Schedule 6 of the Bill increase in the maximum penalty applying to the offences of unauthorised communication of certain information in subsections 18(2) of the ASIO Act and sections 39, 39A and 40 of the IS Act to 10 years' imprisonment (from two years' imprisonment).[90]

266. The Explanatory Memorandum notes that these amendments are necessary as:

> *…the present maximum penalty applying to these offences (being two years' imprisonment) is disproportionate to the significant, adverse consequences that the unauthorised disclosure of highly classified information can have on a country's reputation, intelligence-sharing relationships and intelligence-gathering capabilities. A higher maximum penalty is needed to reflect the gravity of the wrongdoing inherent in such conduct in the contemporary security environment. (p 129)*

267. The Law Council acknowledges the risk of serious harm to intelligence and security interests that is occasioned by unauthorised disclosure of security intelligence-related information. It also acknowledges safeguards in the Bill which include for example: the commencement of a prosecution requires the consent of the Attorney-General who may have regard to broader public policy considerations;[91] the limited lawful communications provisions for instance in Division 1 of Part III of the ASIO Act; and subsection 18(9) of the IGIS Act will apply which provides that a person is not liable to penalty under any law of the Commonwealth or of a Territory by reason only of the person having given information, produced a document, or answered a question when required to do so in accordance with a written notice issued by the IGIS under subsection 18(1) of the IGIS Act.

268. The Law Council notes that these measures are subject to the public interest disclosure scheme contained in the *Public Interest Disclosure Act 2013* (Cth). However, given the very limited circumstances in which this legislation may apply in an intelligence context (discussed above), the Law Council urges the Committee to consider whether these limited protections are sufficient.

269. Further, the Law Council notes that the increased penalty does not appear to be consistent with similar provisions relating to unauthorised disclosure of information. For example, section 70 of the Crimes Act apply criminal sanctions to the breach of secrecy obligations by public officials but only carries a penalty of two years' imprisonment. The Law Council queries whether an unauthorised disclosure of information for example by a member of the AFP should be less criminally culpable than disclosure by an AIC employee or ASIO affiliate.

270. As noted above, the Law Council also encourages the PJCIS to consider whether the increase is necessary in light of such conduct potentially being captured by

[89] Explanatory Memorandum to the NSLA Bill, p 129.
[90] Current subsections 18(2) of the ASIO Act and sections 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth) make it an offence for an unauthorised communication of certain information by ASIO and Australia's foreign intelligence agency officers.
[91] See for example proposed section 18C of the ASIO Act as contained in the NSLA Bill.

terrorism offences;[92] intentionally or recklessly causing harm to Australians overseas;[93] treason offences;[94] espionage offences;[95] secrecy offences in the Crimes Act;[96] and secrecy offences for employees of IS Act organisations.

271. The Law Council considers that if an increase in penalty is considered necessary, an alternative option that the Law Council recommends the PJCIS consider would be whether an additional safeguard should be implemented, namely that an additional physical element of the offence should apply relating to a result that the information disclosed is or is likely to be prejudicial to national security. This would require the prosecution to prove that a person was aware of a substantial risk that the relevant disclosure is or is likely to be prejudicial to national security, and that he or she nonetheless, and unjustifiably in the circumstances known to him or her, took that risk by disclosing the information.

Extension of the unauthorised communication offences in the IS Act to additional AIC agencies

272. Schedule 6 also extends the unauthorised communication offences in sections 39, 39A and 40 of the IS Act to additional agencies within the AIC, namely ONA and the DIO.

273. The Law Council considers that such an extension is appropriate given that ONA and DIO are essential AIC agencies. It also supports efforts to ensure that Commonwealth legislation is consistent in this area.

Unauthorised dealings with certain records of an intelligence agency

274. In addition, the Bill includes new offences in respect of intentional unauthorised dealings with certain records of an intelligence agency, where those deals stop short of the unauthorised communication of information to a third party, for example, the intentional unauthorised removal, retention, copying or transcription of a record. These new offences apply to persons who have accessed certain information of ASIO or an IS Act agency while acting in a specified official capacity and who deal with this information without authorisation. The offences carry a maximum penalty of three years' imprisonment.[97]

275. The Explanatory Memorandum notes that:

> *The creation of an unauthorised dealing offence is necessary to address the current legislative gap in existing protections for conduct that carries a significant risk of jeopardising Australia's national security but stops short of communication of that information to third parties. There is an inherent harm*

[92] Including: Division 101 of the Criminal Code – particularly given the definition of terrorism in section 100.1 of the Criminal Code and offences for example for committing a terrorist act and the pre-emptive offences which apply to the early stages of preparing for a terrorist act, including possessing things connected with terrorist acts (section 101.4), collecting or making documents likely to facilitate terrorist acts (section 101.5) and doing any other act in preparation of a terrorist act (section 101.6); and Division 102 of the Criminal Code which makes it an offence to intentionally provide support or resources to a terrorist organisation.
[93] Division 115 of the Criminal Code.
[94] Division 80 of the Criminal Code.
[95] Section 91.1 of the Criminal Code.
[96] Including: section 70 of the Crimes Act makes it an offence for current or former Commonwealth officers to disclose any facts they have learned or documents they have obtained by virtue of being a Commonwealth officer and which it is their duty not to disclose; and section 79 of the Crimes Act which sets out multiple offences where a person communicates official secrets.
[97] Proposed section 18A of the ASIO Act and sections 40C, 40E, 40G, 40J and 40L of the IS Act.

in placing the particular type of information held by those agencies at risk. This offence will apply to all members of the Australian Intelligence Community and to information peculiar to these roles. Members of intelligence agencies are in a unique position of trust and power, and receive often highly classified, information for the purpose of performing official duties and are aware of the procedures of handling such information and the consequences of disclosing that information. Given this, there is a strong and legitimate expectation that those persons will handle that information lawfully – that is, in strict accordance with their authority – at all times.[98]

276. The Law Council understands the danger posed by unauthorised dealings in placing AIC information at risk as this has the potential to cause considerable harm to Australia's national security interests. However, the Law Council notes that this proposal has not received full consultation on whether determination of a criminal charge in such circumstances is appropriate.

277. In particular, the Law Council is concerned that the offence captures a wide range of conduct which does not require that the unauthorised dealing involves or is likely to involve considerable harm to Australia's national security interests. It may for instance capture conduct of an ASIO employee who takes work home for the purposes of meeting a deadline. Such an action should not be condoned and should carry consequences. However, the Law Council queries whether a person should be held liable to three years' imprisonment on the basis of such conduct.

278. There does not appear to have been a consideration of whether other mechanisms for imposing liability on such conduct, such as the removal of a security clearance or a position of authority would be more appropriate.

279. Further, the offences do not require that the person removed, retained, copied or transcribed a record or otherwise dealt with a record with an intention to endanger or release the information.

280. Accordingly, the Law Council encourages the PJCIS to obtain the views of the INSLM, who could report on the operation, implications and effectiveness of existing offences, before recommending such offences be enacted.

281. If contrary to the Law Council's proposal, the offence is to be progressed, an alternative option that the Law Council recommends the PJCIS consider would be whether an additional safeguard should be implemented, namely that an additional physical element of the offence should apply relating to a result that the unauthorised dealing is or is likely to be prejudicial to national security. This would require the prosecution to prove that a person was aware of a substantial risk that the relevant dealing is or is likely to be prejudicial to national security, and that he or she nonetheless, and unjustifiably in the circumstances known to him or her, took that risk by engaging in the unauthorised dealing.

Unauthorised recording of certain information

282. The Bill also includes new offences in respect of the intentional unauthorised recording of certain information or matter. These offences carry a maximum penalty of three years' imprisonment.[99]

[98] Explanatory Memorandum to the NSLA Bill, pp 30-31.
[99] Proposed section 18B of the ASIO Act and sections 40D, 40F, 40H, 40K and 40M of the IS Act.

283. Currently, the Law Council considers that such offences have not been demonstrated to be necessary and therefore they should not be enacted.

284. The Explanatory Memorandum to the Bill notes that the new offences cover the 'intentional unauthorised making of records of information or matters in connection with, or relating to, the Organisation's performance of its statutory functions'. The offences apply to an 'entrusted person' as a person who is an ASIO employee, an ASIO affiliate (as these terms are defined in section 4) or any other person who has entered into a contract, agreement or arrangement with ASIO, otherwise than as an ASIO affiliate.[100]

285. The circumstances in which an entrusted person may make an unauthorised recording are unclear. The Explanatory Memorandum does not appear to provide examples where an unauthorised recording may occur, or has occurred.

286. The Law Council is concerned that the offence captures a wide range of conduct which does not require that the unauthorised recording involves or is likely to involve considerable harm to Australia's national security interests. That is, the NSLA Bill does it establish a sufficient nexus between such action and any potential risk to compromising Australia's national security interests.

287. The Law Council queries for instance whether it would capture conduct of an ASIO employee who during a meeting with various ASIO sections or divisions takes notes which include some that are not directly related to the specific work of the ASIO employee. The employee may have taken the notes however simply to understand the issues better in order to more fully participate in the meetings to which he or she was invited to attend. A person should not be held liable to three years' imprisonment on the basis of such conduct.

288. The Law Council encourages the PJCIS to inquire further into these matters before making a determination as to the necessity of the offences.

289. It also notes that the utility of the offence may be compromised by difficulties in the prosecution proving that the record is not made by the person as an AIC employee in the course of the person's duties as such an employee or an ASIO affiliate in accordance with the contract, agreement or other arrangement under which the person is performing functions or services for example ASIO.

290. Accordingly, the Law Council encourages the PJCIS to obtain the views of the INSLM, who could report on the operation, implications and effectiveness of existing offences, before recommending such offences be enacted.

291. If contrary to the Law Council's proposal, the offence is to be progressed, an alternative option that the Law Council recommends the PJCIS consider would be whether an additional safeguard should be implemented, namely that an additional physical element of the offence should apply relating to a result that the unauthorised recording is or is likely to be prejudicial to national security. This would require the prosecution to prove that a person was aware of a substantial risk that the relevant dealing is or is likely to be prejudicial to national security, and that he or she nonetheless, and unjustifiably in the circumstances known to him or her, took that risk by engaging in the unauthorised dealing.

[100] Proposed subsections 18B(5) and 18A(5)) of the ASIO Act.

Conclusion

292. The NSLA Bill constitutes the most significant modification to Australia's anti-terrorism laws since the introduction of control orders and preventative detention orders in late 2005 in response to the 7 July 2005 London bombings. It is designed to strengthen the legislative framework governing the activities of Australia's intelligence agencies to respond to threats to Australia's national security emerging from Australians engaged in conflicts overseas and disclosures of classified intelligence information. However, it contains a number of measures with the potential to impact significantly on the rights and freedoms of Australians.

293. The Law Council therefore considers that the newly appointed INSLM should be asked to consider the operation, implications and effectiveness of existing legislation, with a view to addressing the issues which are raised in the Bill, prior to its passage. Such a review would enable all the relevant agencies likely to use these laws to provide further detailed information and examples of how they will work in practice and what benefits they will provide in terms of the protection of Australia's national security. It would also enable organisations such as the Law Council to provide further detailed comments on what impact some of these changes may have on the rights of ordinary Australians, to undertake comparative law analysis where relevant and to explore alternative options for achieving the stated aims of the reforms.

294. If, contrary to the Law Council's recommendation, the PJCIS considers that the NSLA Bill should be enacted without further consultation, the Law Council encourages the Committee to recommend that the safeguards in the Bill be strengthened in a manner suggested by the Law Council in this submission.

Attachment A: Profile of 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 Large Law Firm Group, 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
- The Large Law Firm Group (LLFG)
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of approximately 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 2014 Executive are:

- Mr Michael Colbran QC, President
- Mr Duncan McConnel President-Elect
- Ms Leanne Topfer, Treasurer
- Ms Fiona McLeod SC, Executive Member
- Mr Justin Dowd, Executive Member
- Dr Christopher Kendall, Executive Member

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