2

The National Security Legislation Amendment Bill (No.1) 2014

Introduction

2.1 The chapter contains:

- an overview of the content of the National Security Legislation Amendment Bill (No.1) 2014 (the Bill)
- more detailed information on the provisions of each of the seven schedules to the Bill and their relationship to the previous Committee's recommendations, and
- a brief summary of measures that were proposed during the previous Committee's inquiry and its report but are not reflected in the Bill.

Summary of measures in the Bill

2.2 The National Security Legislation Amendment Bill (No.1) 2014 (the Bill) was introduced into the Senate by the Attorney-General on 16 July 2014.

2.3 In a submission to the inquiry, the Attorney-General's Department (the Department) advised that the Bill would implement 18 of the Committee's 22 recommendations in full, and three recommendations in part.[1] The

1 Attorney-General's Department, *Submission 1*, p. 2.

submission also contained a table which outlined in further detail the position adopted in the Bill towards each of the recommendations.

2.4 The Department outlined that the Bill, if passed, would primarily amend the *Australian Security Intelligence Act 1979* (the ASIO Act) and the *Intelligence Services Act 2001* (the IS Act) in seven key areas:

- Modernising the Australian Security Intelligence Organisation's (ASIO) statutory employment framework (Schedule 1)
- Modernising and streamlining ASIO's warrant-based intelligence collection powers (Schedule 2)
- Strengthening ASIO's capability to conduct covert intelligence operations subject to appropriate safeguards and oversight (Schedule 3)
- Clarifying and improving the statutory framework for ASIO's co-operative and information-sharing activities (Schedule 4)
- Enhancing the capabilities of agencies under the Intelligence Services Act (Schedule 5)
- Improving protection of intelligence-related information (Schedule 6), and
- Renaming of Defence agencies to better reflect their roles (Schedule 7).[2]

2.5 The Department's submission highlighted that, in addition to responding to the Committee's previous recommendations, the Bill contains five additional measures:

- additional amendments to employment provisions relating to ASIO, including to provide for voluntary moves to the Australian Public Service (Item 19 in Schedule 1– new section 89) and consolidating the various terminology used in the ASIO Act and across the Commonwealth statute book to describe persons employed by ASIO or performing functions or services for ASIO in accordance with a contract, agreement or other arrangement (Item 4 of Schedule 1)
- the extension of immunity for actions preparatory or ancillary to an overseas activity of an agency under the Intelligence Services Act (Item 12 of Schedule 5 amending subsection 14(2) of the Intelligence Services Act)
- clarifying that an ASIS staff member or agent can use a weapon or self-defence technique in a controlled environment, like a gun club, a firing range or a martial arts club, where it would be lawful for any other Commonwealth officer and/or member of the public to engage in that activity and where the use would

2 Attorney-General's Department, *Submission 1*, pp. 2–3.

otherwise be consistent with proper performance of an ASIS function

- amendments to the secrecy offences in relation to staff, employees or persons under a contract, agreement or arrangement with ASIO or an agency under the Intelligence Services Act or persons having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIO or an agency under the Intelligence Services Act (Schedule 6) in three ways:
  - ⇒ increasing penalties for the existing unauthorised communication offences in the ASIO Act and the Intelligence Services Act from two years' imprisonment to 10 years' imprisonment
  - ⇒ extending the existing Intelligence Services Act disclosure offences to cover the Defence Intelligence Organisation and the Office of National Assessments and to ensure that all offences cover information received by the agency as well as prepared by it, and
  - ⇒ creating new offences in relation to unauthorised dealings with records and unauthorised recording of information (with a maximum penalty of three years' imprisonment)
- renaming the Defence Imagery and Geospatial Organisation as the Australian Geospatial-Intelligence Organisation (AGO) and the Defence Signals Directorate as the Australian Signals Directorate (ASD) (Schedule 7) and providing a specific function for the IGIS to report on the extent to which the AGO complies with rules made under section 15 of the Intelligence Services Act (Item 134 of Schedule 7).[3]

2.6 Further details on the items included in each of the Bill's seven schedules, including their relationship to the previous Committee's 2013 recommendations, are included on the following pages.

Schedule 1 – ASIO employment etc.

ASIO employment provisions

2.7 The terms of reference for the previous Committee's inquiry into potential reforms of national security legislation indicated that the Government wished to modernise the ASIO Act employment provisions. The proposed reforms included amending the requirement for ASIO employees to hold an 'office'; using a consistent descriptor to denote employees of ASIO;

3 Attorney-General's Department, *Submission 1*, p. 3.

modernising the Director-General's powers in relation to employment terms and conditions; removing an outdated employment provision; and providing additional scope for further secondment arrangements.[4]

2.8 The previous Committee made no comment in its 2013 report on the majority of these changes, noting their apparent 'innocuous and administrative' character.[5] However, regarding the proposed new secondment provisions, the Committee indicated that it was satisfied with those arrangements provided they could not be used 'for the purpose of officers of agencies circumventing existing safeguards and limitations that apply to their employment and conduct'.[6] The Committee made the following recommendation:

> **Recommendation 26:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to modernise the Act's provisions regarding secondment arrangements.

2.9 According to the Explanatory Memorandum, Schedule 1 to the Bill is intended to:

> … modernise the employment provisions contained in Part V of the ASIO Act, to amongst other things, more closely align the provisions with the Australian Public Service (APS) employment framework.[7]

2.10 The Bill includes measures to:

> (a) provide for the Director-General of Security (Director-General) to employ persons as employees, under the concept of a level, rather than as officers holding an 'office'
>
> (b) provide for consistency in the differing descriptors of persons who work within ASIO
>
> (c) modernise the Director-General's powers in relation to employment terms and conditions
>
> (d) provide for secondment arrangements, and

4 Attorney-General's Department, *Equipping Australia against Emerging and Evolving Threats*, July 2012, pp. 8–9.

5 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 104.

6 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, pp. 105–06.

7 National Security Legislation Amendment Bill (No. 1) 2014 (NSLA Bill), *Explanatory Memorandum*, p. 36.

> (e) include provisions to facilitate the transfer of ASIO employees into [Australian Public Service] agencies.[8]

2.11 The first four of these measures (a to d) were, for the most part, covered in the terms of reference for the previous Committee's inquiry, whilst the fifth (e) —provisions for the voluntary moves by employees into the Australian Public Service (APS)—is an additional measure.

2.12 It should also be noted that measure (b) above has been expanded in the Bill to introduce the term 'ASIO Affiliate', defined as a person 'performing functions or service for the Organisation in accordance with a contract, agreement or other arrangement'.[9]

2.13 The Bill (item 19) proposes to create new sections 86 and 87 for the secondment of employees from and to ASIO respectively. Proposed section 87, concerning the secondment of persons *to* ASIO, stipulates that secondees would 'perform services in connection with the performance or exercise of any of the Organisation's functions or powers'. Proposed section 86, concerning the secondments of employees *from* ASIO to other organisations, does not include this restriction. However, the Explanatory Memorandum states that:

> While an ASIO employee would remain an ASIO employee for the duration of the secondment, his or her duties would be those assigned by the body or organisation for whom the ASIO employee is directed to work (or as specified in the written agreement with the Director-General) and would be performed in accordance with the body or organisation's legal or legislative requirements.[10]

2.14 Voluntary moves by employees of ASIO to the APS are supported in the Bill (also through item 19) by proposed new section 89. According to the Explanatory Memorandum, the effect of this provision would be that an ASIO employee who voluntarily moved to an APS agency would be treated as if they were an APS employee, enabling their move to be facilitated by section 26 of the *Public Service Act 1999*.[11]

8 NSLA Bill, *Explanatory Memorandum*, p. 36.

9 Attorney-General's Department, *Submission 1*, p. 26.

10 NSLA Bill, *Explanatory Memorandum*, p. 43.

11 NSLA Bill, *Explanatory Memorandum*, p. 44.

Schedule 2 – Powers of the Organisation

Introduction

2.15 Schedule 2 to the Bill amends the warrant provisions in the ASIO Act, including search warrants, computer access warrants, listening and tracking device warrants and the power to inspect postal or delivery service articles. According to the Explanatory Memorandum, the intent of the changes is to 'to address a number of practical difficulties identified in the powers (special powers) that ASIO can use under warrant in carrying out its statutory functions':

> Although there have been several amendments to these powers in the past, the amendments have been piecemeal and have not kept pace with technological advancements. To maintain effective intelligence gathering techniques and capabilities, ASIO's powers require modernising to provide a statutory framework which facilitates intelligence collection by the most technologically effective and efficient means. These amendments will provide ASIO with improved statutory powers to uphold Australia's vital national security interests.[12]

2.16 The proposed amendments to the warrant provisions are largely in line with those that were examined in the Committee's previous inquiry. Further detail on how the proposed amendments relate to the Committee's previous recommendations is provided below.

Computer access warrants – definition of computer

2.17 In its 2013 report, the Committee supported a proposal to update the definition of a computer in the ASIO Act to include computer networks. The Committee also supported updating the provisions for computer access warrants to enable ASIO to access all computers at a particular location or associated with a nominated person.[13] The Committee made the following recommendation:

> **Recommendation 20:** The Committee recommends that the definition of computer in the *Australian Security Intelligence Organisation Act 1979* be amended by adding to the existing definition the words "and includes multiple computers operating in a network".

12 NSLA Bill, *Explanatory Memorandum*, p. 63.

13 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, pp. 88–89.

> The Committee further recommends 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.

2.18 The Bill implements this recommendation through amendments to section 22 and section 25A of the ASIO Act (items 4 and 18), although different wording was selected. The updated provisions are intended to 'clarif[y] the ambiguity' in the existing computer definition and to enable warrant provisions to 'better reflect the way people use computer technology in the modern world'.[14]

Search and computer access warrants – disruption of target computer

2.19 In its 2013 report, the previous Committee gave qualified support to a proposal to amend the ASIO Act provisions on computer access warrants to stipulate that the existing prohibition on disrupting computers does not apply to activities that would be necessary to execute the warrant. The Committee encouraged the Government to consider including provisions in the ASIO Act that would prevent damage or cause loss to telecommunications systems operated by third parties.

2.20 The Committee also endorsed comments by the Inspector General of Intelligence and Security (IGIS) that the amendments would need to be framed carefully to balance the 'potential consequences of this interference to the individual(s) with the threat to security', and that there should be appropriate review and oversight mechanisms with particular attention to the effect of any disruption on third parties.[15] The Committee made the following recommendation:

> **Recommendation 21:** The Committee recommends that the Government give further consideration to amending the warrant provisions in the *Australian Security Intelligence Organisation Act 1979* to enable the disruption of a target computer for the purposes of executing 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.

14 NSLA Bill, *Explanatory Memorandum*, pp. 64, 69.

15 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, pp. 91–92.

2.21 The Bill (items 12 and 25) implements the Government's response to this recommendation by proposing to replace the existing subsections 25(6) and 25A(5) of the ASIO Act. The intent of the proposed amendments is to 'address the difficulties in executing … warrants caused by advancements in technology'. The amendments apply both to computer access warrants and to search warrants for which the Minister has authorised the use of a computer to access data.[16]

2.22 The existing subsections prohibit ASIO from doing anything that interrupts, interferes with or obstructs the lawful use of a computer, or causes any loss or damage to other persons during the execution of the warrant. The proposed modified subsections would reduce these restrictions on ASIO's warrant powers by only prohibiting actions that *materially* interfere with, interrupt or obstruct lawful use of a computer, and adding an exception to this prohibition for when the action is necessary in order to execute the warrant. The modified subsections would also only prohibit actions that caused *material* loss or damage to other persons.[17]

Computer access warrants – access to third party computers

2.23 In its 2013 report, the previous Committee supported the necessity, in certain circumstances, for ASIO to be able to access a third party computer or communication in transit for the purpose of gaining access to a target computer, noting that this new power would align with existing powers under the *Telecommunications (Interception and Access) Act 1979*. The Committee also noted the significant privacy implications of this proposed new ability, and emphasised the need for appropriate safeguards and accountability mechanisms to be in place.[18] The Committee made the following recommendation:

> **Recommendation 22:** The Committee recommends that the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the *Telecommunications (Interception and Access) Act 1979*.

16 NSLA Bill, *Explanatory Memorandum*, pp. 67, 72.

17 NSLA Bill, *Explanatory Memorandum*, pp. 67, 71–72.

18 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 95.

2.24 This measure is primarily implemented through a proposed amendment to subsection 25A(4) of the ASIO Act (item 23 of the Bill). The amendment would enable ASIO to use a third party computer or 'communication in transit' in order to access data held on a target computer. If necessary to achieve the purpose, ASIO would also be able to add, copy, delete or alter data on the third party computer or communication in transit. The intent of the amendments is to 'keep track with technological developments which have made it increasingly difficult for ASIO to execute its computer access warrants'.[19]

2.25 The proposed new paragraph includes a safeguard that the use of the third party computer or communication in transit will need to be 'reasonable in all the circumstances, having regard to any other methods of obtaining access to the data held in the target computer which are likely to be as effective'.[20]

2.26 As an additional safeguard, the Bill (item 46) also proposes to insert a new section into the ASIO Act to clarify that nothing in ASIO's warrant powers relating to computers and communications in transit authorises the interception of a communication for the purposes of the *Telecommunications (Interception and Access) Act 1979*, which would require a separate warrant application.[21]

Variation of warrants

2.27 The previous Committee accepted a proposal to allow for active warrants under the ASIO Act to be varied, noting that appropriate accountability would be maintained if such variation was authorised by the Attorney-General.[22] The Committee made the following recommendation:

> **Recommendation 23:** The Committee recommends the Government amend the warrant provisions of the *Australian Security Intelligence Organisation Act 1979* to promote consistency by allowing the Attorney-General to vary all types of ASIO Act warrants.

2.28 The Bill (item 44) implements this recommendation by proposing the insertion of new section 29A into the ASIO Act to enable the Attorney-General to vary the terms of warrants, with the exception of emergency warrants, at the request of the Director-General of Security. The Director-

19 NSLA Bill, *Explanatory Memorandum*, p. 71.

20 NSLA Bill, *Explanatory Memorandum*, p. 71.

21 NSLA Bill, *Explanatory Memorandum*, p. 93.

22 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 98.

General would be required to specify the grounds on which the request for variation was being made. If a variation included an extension to the period of time in which the warrant was in force, the total time in force would not be able to exceed the maximum periods specified elsewhere in the Act.

2.29 The Explanatory Memorandum states that this power would 'only be used for variations of a relatively minor nature', and that a new warrant would be sought for more significant changes.[23]

Identified person warrants

2.30 In its 2013 report, the previous Committee examined a proposal for ASIO and the Attorney-General to be able to issue a single warrant to authorise the use of multiple powers, over one person, for the same investigatory purpose. The Committee noted that the proposal was not intended to weaken any of the thresholds for the use of the various special powers, and that the Attorney-General would have to decide which particular powers would be covered by each warrant.

2.31 The previous Committee considered that while, in this instance, the classified evidence it received was 'sufficient to give in principle support to the proposal', further examination of the proposal would be necessary.[24] It made the following recommendation:

> **Recommendation 29:** The Committee recommends that should the Government proceed with amending the *Australian Security Intelligence Organisation Act 1979* 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.

2.32 The Bill (item 41) proposes to insert a new subdivision into the ASIO Act to allow for an 'identified person warrant' to be issued. As had been proposed, this would enable the Attorney-General to issue a single warrant to authorise the use of multiple powers to collect intelligence on an identified person. To issue an identified person warrant, the Attorney-General would be required to be satisfied both that:

23 NSLA Bill, *Explanatory Memorandum*, p. 92.

24 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 114.

- the identified person is 'engaged in or is reasonably suspected by the Director-General of being engaged in, or likely to engage in, activities prejudicial to security'; and
- issuing an identified person warrant would, or would be likely to, 'substantially assist the collection of intelligence relevant to security'.[25]

2.33 ASIO would also require further specific authorisation from either the Attorney-General or the Director-General before exercising any of the powers listed on the identified person warrant, subject to a threshold test. The Explanatory Memorandum notes that the test for authorisations under an identified person warrant would be 'more stringent than the various tests that currently apply to the issuing of warrants authorising ASIO to do comparable things' in other parts of the Act.

2.34 The Explanatory Memorandum further explains that the identified person warrant would be subject to the same, or stricter, safeguards as other existing warrants, including issuing thresholds, maximum durations, accountability mechanisms and oversight arrangements.[26]

Surveillance device warrants

2.35 In its 2013 report, the previous Committee accepted a proposal to align the surveillance device provisions in the ASIO Act with the more modern *Surveillance Devices Act 2004*, which provides for warrants for the use of surveillance devices by law enforcement agencies. The Committee noted that the IGIS did not have concerns with the proposal if it was limited to modernising the language of the ASIO Act. The Committee recommended the following:[27]

> **Recommendation 30:** The Committee recommends that the *Australian Security Intelligence Organisation 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.

2.36 The Bill (item 29) proposes to introduce a new framework, based on the *Surveillance Devices Act 2004*, to regulate ASIO's use of surveillance devices such as listening devices, tracking devices, and optical surveillance devices.

25 NSLA Bill, *Explanatory Memorandum*, p. 81.

26 NSLA Bill, *Explanatory Memorandum*, pp. 82-83.

27 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, pp. 115–116.

2.37 The framework includes introducing a single surveillance device warrant authorising the use of multiple numbers, combinations and types of devices (excluding data surveillance devices) in relation to a particular person, premises, object or class of objects. The warrant would be issued by the Minister and subject to the same thresholds that currently exist under the ASIO Act. The proposed new framework also removes an existing general prohibition on ASIO's use of listening devices, tracking devices and optical surveillance devices, and identifies circumstances under which they can be used without a warrant. For example, an optical surveillance device would be able to be used without a warrant if it did not involve entering the target's premises or interfering with their vehicle without permission (proposed section 26D).[28]

2.38 As a safeguard, the proposed new framework allows for the Director-General of Security to exclude certain ASIO affiliates from the power to use surveillance devices without a warrant, 'where appropriate for operational reasons, or in the interests of national security'.[29]

Execution of warrants – authorisation by class of person

2.39 The previous Committee concluded that there was no clear benefit in maintaining the current requirement to specifically name ASIO officers who are authorised to execute warrants, and accepted the rationale for moving to authorising ASIO officers by position rather than specific name. The Committee made the following recommendation:

> **Recommendation 32:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to establish classes of persons able to execute warrants.

2.40 The Bill (item 8) proposes to implement this recommendation by replacing the existing section 2 of the ASIO Act to provide that the Director-General (or a senior position-holder authorised by the Director-General) may approve a person or class of persons to exercise the authority of a warrant under the Act. The intent of the measure is to address the 'operational inefficiency' that results from requiring ASIO to maintain a named list of individuals involved in exercising authority under a warrant, which may be taking place in 'unpredictable and volatile environments'.[30]

28 NSLA Bill, *Explanatory Memorandum*, pp. 73–74.

29 NSLA Bill, *Explanatory Memorandum*, p. 78.

30 NSLA Bill, *Explanatory Memorandum*, pp. 65–66.

Search and computer access warrants – access to third party premises

2.41 In its 2013 inquiry, the previous Committee examined a proposal to amend the ASIO Act to clarify the authority of ASIO officers to access third party premises to execute a warrant on an incidental basis. The Committee noted that it shared 'community concerns that the existing incidental entry power might lead to arbitrary interference with an innocent person's home or property'. However, noting that there may be a need for incidental entry onto premises to give effect to ASIO warrants in some limited circumstances, the Committee accepted that the proposal would not lead to the arbitrary interference as the scheme was intended to 'operate with requirements of proportionality and using as little intrusion into privacy as possible'.[31] The Committee recommended:

> **Recommendation 35:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* 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. However, the Committee is of the view that whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.

2.42 The Bill (items 10 and 19) implements the proposal by inserting new paragraphs into the provisions for search and computer access warrants to 'make it clear that third party premises can be entered in order to gain entry to or exit the subject premises for the purposes of executing a search warrant'. The Explanatory Memorandum describes examples in which this power could be relied upon, such as: when there is no other way to access the subject premises; when entry through an adjacent premises is operationally preferable; and in emergency circumstances.[32]

Execution of warrants – use of reasonable force

2.43 In its 2013 report, the previous Committee supported a proposal to clarify that reasonable force may be used at any time during the execution of a search warrant, not just on entry. The Committee emphasised that the purpose of the proposal was 'not to authorise the use of force against a

31 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 127.

32 NSLA Bill, *Explanatory Memorandum*, pp. 66, 69.

person, but against property in order to facilitate the conduct of the search'.[33] It made the following recommendation:

> **Recommendation 36:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.

2.44 The Bill implements the proposal through amendments to the ASIO Act's provisions for various types of warrants to clarify that 'the use of force that is necessary and reasonable to do the things specified in the warrant is not limited to entry, but can be used at any time during the execution of the warrant'.[34]

2.45 The Government did not agree with the previous Committee's recommendation that use of reasonable force against a person should be excluded.[35] As such, the Bill includes amendments to specify that force may be used 'against persons and things'. The Explanatory Memorandum notes that the use of force against a person would be subject to strict safeguards, including that it could only be used where it was 'necessary and reasonable to do the things specified in a warrant for the purposes of executing that warrant', such as when a person is 'seeking to obstruct an ASIO employee in the execution of a warrant'. Further, use of force against a person outside these requirements 'may attract criminal and civil liability'.[36]

Evidentiary certificate regime

2.46 In its 2013 report, the previous Committee agreed with a proposal to introduce an evidentiary certificate regime to protect the identities of officers and sensitive capabilities of ASIO involved in the execution of warrants. The Committee further suggested that there should be a limit on the extent to which evidentiary certificates could be utilised, in that they could be used to prove the validity of how information was obtained, but not whether the information itself was true. The Committee concluded that

33 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, pp. 129–130.

34 NSLA Bill, *Explanatory Memorandum*, p. 68.

35 Attorney-General's Department, *Submission 1*, p. 17.

36 NSLA Bill, *Explanatory Memorandum*, p. 68.

> the evidentiary certificate scheme should be drafted in a way such that ultimate facts are not to be the subject of an evidentiary certificate, and that the content of such a certificate would be limited to certain technical facts removed from a fact in issue before a court.[37]

2.47 The Committee made the following recommendation:

> **Recommendation 37:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to introduce an evidentiary certificate regime to protect the identity of officers and sources. The Committee also recommends that similar protections be extended to ASIO in order to protect from disclosure in open court its sensitive operational capabilities, analogous to the provisions of the *Telecommunications (Interception and Access) Act 1979* and the protections contained in the counter terrorism provisions in the Commonwealth Criminal code.
>
> The Committee further recommends that the Attorney-General give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.

2.48 The Bill (item 47) proposes to implement an evidentiary certificate regime by adding new section 34AA to the ASIO Act. The Explanatory Memorandum states that the regime would work in a similar fashion to existing schemes in the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*. The regime would allow the Director-General (or Deputy Director-General) of Security to issue an evidentiary certificate with respect to acts or things done in connection with a computer access warrant or surveillance device warrant (and with other warrants in more limited circumstances).[38]

2.49 The Explanatory Memorandum advises that, under the proposed regime, evidentiary certificates will 'only cover the manner in which the evidence was obtained … and not the evidence itself'.[39]

37 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 131.

38 NSLA Bill, *Explanatory Memorandum*, p. 93.

39 NSLA Bill, *Explanatory Memorandum*, p. 94.

Schedule 3 – Protection for special intelligence operations

Special intelligence operations

2.50 In its 2013 report, the previous Committee accepted a proposal to amend the ASIO Act to create a controlled intelligence operations scheme, subject to strict accountability and oversight, which would authorise ASIO officers and sources to engage in conduct which may, in ordinary circumstances, be a breach of the criminal law. The Committee understood that the occasions on which such a scheme would be used 'would be seldom but may from time to time arise', and supported the adaptation of the procedures and safeguards in *Crimes Act 1914* that applied to the Australian Federal Police (AFP)'s 'controlled operations'. The effect would to be exempt ASIO officers and agents from criminal and civil liability only for certain authorised conduct, while unreasonable or reckless conduct would not be indemnified.[40] The Committee made the following recommendation:

> **Recommendation 28:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the *Crimes Act 1914*.

2.51 The Bill proposes to implement this recommendation by introducing into the ASIO Act a statutory framework for the conduct of 'special intelligence operations' (SIOs). The SIO scheme is 'based broadly' on the controlled operations scheme in the *Crimes Act 1914*, although 'appropriate modifications have been made to reflect the differences between a law enforcement operation … and a covert intelligence-gathering operation'.[41]

2.52 The intent of the scheme is to 'ensure ASIO officers, employees and agents will have appropriate legal protections when conducting covert operations', for example, if an ASIO officer were to attend, as part of a covert operation, a training session provided by a terrorist organisation. The Explanatory Memorandum notes that 'at present, some significant covert operations either do not commence or are ceased due to the risk that participants could be exposed to criminal or civil liability'.[42]

---

40 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 111.

41 NSLA Bill, *Explanatory Memorandum*, p. 96.

42 NSLA Bill, *Explanatory Memorandum*, pp. 96–97.

2.53 The commencement of an SIO would be subject to authorisation by the Director-General or Deputy Director General of Security. Authorisation of an SIO would be subject to criteria outlined in proposed section 35C , including that any unlawful conduct under the SIO would be 'limited to the maximum extent' and would not include causing death or serious injury to a person, committing a sexual offence, or causing significant loss or damage to property. The immunity provided under the scheme would be limited to conduct authorised under the SIO (proposed section 35K). Further, proposed section 35L stipulates that conduct authorised under an SIO would not affect the need to obtain a warrant for certain activities under the ASIO Act or *Telecommunications (Interception and Access) Act 1979*.

2.54 Proposed section 35P creates two offences in relation to unauthorised disclosure of information relating to an SIO. These comprise a basic offence carrying a five year maximum jail term; and an aggravated offence carrying a ten year maximum jail term for cases in which the person endangers, or intends to endanger, the effectiveness of the SIO or the health or safety of those involved. The Explanatory Memorandum makes it clear that these offences could apply to anyone:

> The offences apply to disclosures 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.[43]

2.55 Proposed section 35Q outlines specific reporting requirements for the SIO scheme, comprising six-monthly written reports to the Minister and the IGIS on the extent to which each SIO has assisted ASIO in its functions.

Schedule 4 – ASIO cooperation and information sharing

ASIO cooperation with private sector

2.56 In its 2013 report, the previous Committee offered support to 'amending legislation to give ASIO a clear mandate to cooperate with the private sector'. The Committee noted that it had an open mind as to whether confidentiality issues arising from dealing with the private sector should be addressed by legislation or administrative arrangements. While not making a formal recommendation, in the text of the report the Committee recommended that the Government clarify the types of information that

43 NSLA Bill, *Explanatory Memorandum*, p. 111.

would be shared and what handling and dissemination limitations would apply in legislation.[44] The Committee then made the following recommendation:

> **Recommendation 33:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to formalise ASIO's capacity to co-operate with private sector entities.

2.57 The Bill (item 5) proposes to insert a new paragraph into subsection 19(1) of the ASIO Act to specify that, so far as necessary for, or conducive to, the performance of its functions, ASIO may cooperate with 'any other person or body whether within or outside Australia' in addition to the authorities already listed. The amendment is intended to clarify 'uncertainty as to whether section 19 could be read to exclude ASIO's ability to cooperate with the private sector'. The Explanatory Memorandum notes that ASIO's ability to cooperate with the private sector is 'particularly important' due to the private ownership of large amounts of Australia's critical infrastructure and its vulnerability to security threats.[45]

Referral of section 92 breaches to law enforcement agencies

2.58 Section 92 of the ASIO Act makes it an offence to publish the identity of a current or former ASIO employee or affiliate, carrying a maximum penalty of 12 months imprisonment. In its 2013 report, the previous Committee agreed that there was a need to allow ASIO to refer breaches of section 92 to law enforcement for investigation and made the following recommendation:[46]

> **Recommendation 34:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended so that ASIO may refer breaches of section 92 to law enforcement for investigation.

2.59 The Bill (items 1 to 3) proposes to amend subsection 18(3) of the ASIO Act to specifically allow the Director-General of Security, or a person acting under the Director-General's authority, to communicate information in relation to an offence against section 92. The intention is to overcome a current limitation which prevents such information being communicated because a breach of section 92 does not fall under the definition of a

---

44 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 123.

45 NSLA Bill, *Explanatory Memorandum*, p. 118.

46 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, pp. 124–25.

'serious crime' (for which a maximum sentence of greater than 12 months is required).[47]

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

Clarifying Defence Imagery and Geospatial Organisation functions

2.60 In its 2013 report, the previous Committee agreed that the *Intelligence Services Act 2001* (IS Act) should be amended to clarify the Defence Imagery and Geospatial Organisation (DIGO)'s authority to assist other agencies and bodies, 'provided that the existing oversight and accountability mechanisms would apply'[48], and recommended the following:

> **Recommendation 27:** The Committee recommends that the *Intelligence Services Act 2001* be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.

2.61 The Bill (items 4 and 5) proposes to update the description of DIGO's functions in section 6B of the IS Act to include providing assistance to other agencies in the 'production and use of imagery and other geospatial products' and 'technologies'.[49]

Ministerial authorisation for collecting intelligence on persons undermining ASIS operational integrity

2.62 In its 2013 report, the previous Committee considered a proposal for a new ground to be added to the IS Act to enable Ministerial authorisation for Australia's foreign intelligence organisations to collect intelligence on Australian persons likely to be involved in intelligence or counter-intelligence activities. The Committee supported the addition of such an authorisation into the Act, 'provided that ministerial authorisations would be subject to existing approval mechanisms',[50] and made the following recommendation:

---

47 NSLA Bill, *Explanatory Memorandum*, p. 117.

48 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 108.

49 NSLA Bill, *Explanatory Memorandum*, pp. 119–20.

50 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 134.

Recommendation 38: The Committee recommends that the *Intelligence Services Act 2001* be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.

2.63 The Bill (item 6) proposes to add a new Ministerial authorisation ground to the IS Act 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 the [Australian Secret Intelligence Organisation (ASIS)]'.[51] The 'operational security of ASIS' is defined in the Bill (item 1) as the protection of the integrity of operations of ASIS from 'interference by a foreign power or entity' or 'reliance on inaccurate or false information'.

2.64 The Explanatory Memorandum notes that the existing safeguards in the IS Act would apply to the new ground, including 'the requirements for all authorisations to be made available for inspection by the IGIS'.[52]

ASIS cooperation with ASIO

2.65 In its 2013 report, the previous Committee considered a proposal to amend the IS Act to enable the Minister of an IS Act agency to authorise specified activities which may involve producing intelligence on an Australian person or persons, where that agency is cooperating with ASIO in the performance of an ASIO function.

2.66 Rather than supporting the proposal outlined in the discussion paper for dealing with the inconsistent privacy protections for Australians of interest to both ASIO and a foreign intelligence agency, the Committee agreed with an alternative proposal put forward by the IGIS. This proposal was for an equivalent common standard across the IS Act and the ASIO Act to be introduced for particularly intrusive activities. Noting that where ASIS proposed 'to collect intelligence on an Australian person to assist ASIO with its functions, this would still need to be at the request of ASIO', the Committee recommended the following:[53]

Recommendation 39: The Committee recommends that where ASIO and an *Intelligence Services Act 2001* agency are engaged in a

51 NSLA Bill, *Explanatory Memorandum*, p. 120.

52 NSLA Bill, *Explanatory Memorandum*, p. 120.

53 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, pp. 135–36.

cooperative intelligence operation a common standard based on the standards prescribed in the *Australian Security Intelligence Organisation Act 1979* should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.

2.67 The Bill (item 11) proposes to introduce provisions into the IS Act to enable ASIS to 'undertake a new function of cooperating with ASIO in relation to the production of intelligence on Australian persons in limited circumstances without Ministerial authorisation'.[54] The provisions of the proposed new section 13B stipulate that such cooperation only relates to activity undertaken outside Australia and in support of ASIO in the performance of its functions. A written request from ASIO would be required for ASIS to collect intelligence on a person under this section, except for instances in which an authorised ASIS staff member 'reasonably believes that it is not practicable in the circumstances (like an emergency) for ASIO to notify ASIS' in accordance with this requirement.[55]

2.68 Proposed section 13E of the Bill requires the Director-General of ASIS to be satisfied that the proposed activities under 13B are reasonable and only for the purpose of supporting ASIO. Proposed section 13D stipulates that section 13B powers may not be used to allow ASIS to undertake a particularly intrusive activity overseas that would require a warrant if undertaken in Australia.

2.69 Intelligence produced by ASIS is required, under proposed section 13F, to be communicated to ASIO as soon as practicable. The Explanatory Memorandum notes that this communication would be subject to the existing 'rules to protect the privacy of Australians' under section 15 of the IS Act.[56]

2.70 Under proposed subsection 13B(4), ASIS would be required to notify the IGIS in writing as soon as practicable when it undertakes an activity under section 13B. Section 13F would additionally require ASIS to keep a copy of requests for cooperation that are received from ASIO for inspection on request by the IGIS.

ASIS training in self-defence

2.71 In its 2013 report, the previous Committee indicated that, in its opinion, it was reasonable for ASIS officers to be able to train with its partner

54 NSLA Bill, *Explanatory Memorandum*, p. 119.

55 NSLA Bill, *Explanatory Memorandum*, p. 122.

56 NSLA Bill, *Explanatory Memorandum*, p. 125.

agencies in weapons and self-defence techniques, and 'the lack of such joint training poses an unacceptable danger to ASIS officers and agents'.[57] The Committee made the following recommendation:

> **Recommendation 40:** The Committee recommends that the *Intelligence Services Act 2001* be amended to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

2.72 The Bill (items 9, 14 and 17) proposes to amend the IS Act to allow ASIS to provide weapons, or training in the use of weapons or self-defence techniques, to officers from a 'small number of Australian agencies that have a lawful right under Australian law to carry weapons' and 'staff from a limited number of trusted foreign authorities that are approved by the Foreign Minister after consulting the Prime Minister and Attorney-General'.[58]

Extension of immunity for actions overseas

2.73 Section 14 of the IS Act currently provides limited immunity for acts 'done inside Australia' in connection with the overseas activities of the agencies concerned. The Bill (item 13) proposes to extend this limited immunity to activities outside Australia. The intent of the amendment is to 'ensure that persons who assist the IS Act agencies outside Australia are provided with the same limited protection from Australian law as those persons who assist IS Act agencies in Australia'.[59]

2.74 This proposal was not considered in the previous Committee's 2013 report.

ASIS use of weapons in controlled environments

2.75 The Bill (item 16) proposes to amend the IS Act to allow the use of weapons or self-defence techniques by ASIS officers in a 'controlled environment' (for example, a rifle range or martial arts club) as part of their duties and in compliance with guidelines issued by the Director-General. The intent of the proposed amendment is to clarify that 'ASIS staff members and agents are able to use weapons or self-defence

57 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, pp. 137–138.

58 NSLA Bill, *Explanatory Memorandum*, p. 127.

59 NSLA Bill, *Explanatory Memorandum*, p. 126.

techniques … where it would be lawful for any other Commonwealth officer or member of the public to engage in that activity'.[60]

2.76 This proposal was not considered in the previous Committee's 2013 report.

Schedule 6 – Protection of information

Increased penalties and new offences

2.77 The Bill proposes to amend the secrecy offences in the ASIO Act and IS Act in regards to unauthorised handling and communication of information. The intent of the amendments is

> to ensure that the secrecy offences in the ASIO Act and the IS Act target, denounce and punish appropriately the wrongdoing inherent in the intentional unauthorised communication of, or dealing with, the official records or information of [Australian Intelligence Community] agencies.[61]

2.78 As summarised in the Explanatory Memorandum, the measures in Schedule 6 make four key amendments to both Acts:

- An 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 from two years' imprisonment to 10 years' imprisonment.
- An extension of the unauthorised communication offences in sections 39, 39A and 40 of the IS Act to additional agencies—namely the Office of National Assessments (ONA) and the Defence Intelligence Organisation (DIO) (new sections 40A and 40B).
- New offences for intentional unauthorised dealings with certain records of an intelligence agency that 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 all agencies within the Australian Intelligence Community (AIC) and carry a maximum penalty of three years' imprisonment (new section 18A of the ASIO Act and sections 40C, 40E, 40G, 40J and 40L of the IS Act).

60 NSLA Bill, *Explanatory Memorandum*, p. 127.

61 NSLA Bill, *Explanatory Memorandum*, p. 129.

- New offences for the intentional unauthorised recording of certain information or matter. These offences apply to all AIC agencies and carry a maximum penalty of three years' imprisonment (new section 18B of the ASIO Act and sections 40D, 40F, 40H, 40K and 40M of the IS Act).[62]

2.79 The Explanatory Memorandum explains that the amendments are intended to rectify two 'major limitations' in the coverage of the existing offences:

> 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.[63]

and

> the existing secrecy offences in the ASIO Act and the IS Act focus on the unauthorised communication of information and do not address the wrongdoing associated with any other form of intentional unauthorised dealing with information or records.[64]

2.80 Safeguards identified in the Explanatory Memorandum concerning the amended offence provisions include: the Attorney-General's discretion on whether to proceed with a prosecution; oversight by the IGIS; and immunity for disclosure under the regime set out in the *Public Interest Disclosure Act 2013*.[65]

2.81 These proposed amendments were not considered by the previous Committee in its 2013 report.

Schedule 7 – Renaming of Defence agencies

2.82 The Bill proposes to rename the Defence Imagery and Geospatial Organisation (DIGO) as the Australian Geospatial-Intelligence Organisation (AGO); and to rename the Defence Signals Directorate (DSD) as the Australian Signals Directorate (ASD). The intent of the change is to

62 NSLA Bill, *Explanatory Memorandum*, p. 129.

63 NSLA Bill, *Explanatory Memorandum*, p. 129.

64 NSLA Bill, *Explanatory Memorandum*, p. 130.

65 NSLA Bill, *Explanatory Memorandum*, pp. 131–32.

'better reflect the national roles that those organisations play in support of Australia's security'.[66]

2.83 These proposed amendments were not considered by the previous Committee in its 2013 report.

Proposed measures not reflected in the Bill

Renewal of warrants by the Attorney-General

2.84 In its 2013 report, the previous Committee endorsed a proposal to allow for renewal of warrants, on the condition that the standards and thresholds for obtaining a warrant should not be lowered for the renewal of the very same warrant:

> **Recommendation 25:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* be amended to allow the Attorney-General to renew warrants.

2.85 This recommendation is not reflected in the Bill. In his second reading speech on introducing the Bill into the Senate, the Attorney-General advised that the amendment was 'considered unnecessary'.[67]

Extended duration of warrants

2.86 In its 2013 report, the previous Committee concluded that there was insufficient evidence to justify a proposal to increase the maximum duration of search warrants from 90 days to six months. The Committee made the following recommendation:

> **Recommendation 24:** Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of *Australian Security Intelligence Organisation Act 1979* search warrants not be increased.

2.87 In line with this recommendation, there are no proposed amendments in the Bill to extend the duration of search warrants.

66 NSLA Bill, *Explanatory Memorandum*, p. 166.

67 Senator the Hon George Brandis QC, Attorney-General, *Senate Hansard*, 16 July 2014, p. 66.

Person searches independent of premises searches

2.88 In its 2013 report, the previous Committee did not support a proposal to amend the ASIO Act to enable person searches to be undertaken independently of a premises search, noting its 'serious misgivings about whether this power would take ASIO into the realm of law enforcement and policing'.[68] The Committee made the following recommendation:

> **Recommendation 31:** The Committee recommends that the *Australian Security Intelligence Organisation Act 1979* not be amended to enable person searches to be undertaken independently of a premises search.

2.89 In line with this recommendation, there are no proposed amendments in the Bill to allow for person searches to be undertaken independently of premises searches.

Scrutiny of proposed legislation

2.90 In its 2013 report, the previous Committee made the following recommendation:

> **Recommendation 41:** The Committee recommends that the draft amendments to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*, necessary to give effect to the Committee's recommendations, should be released as an exposure draft for public consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.
>
> In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

2.91 An exposure draft of the Bill was not released for public consultation prior to its introduction into the Senate. However, on the day that it was introduced, the Bill was referred to the Committee to conduct a public inquiry.

---

68 PJCIS, *Report of the inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 119.