The Parliament of the Commonwealth of Australia

Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014

Parliamentary Joint Committee on Intelligence and Security

September 2014
Canberra

ISBN 978-1-74366-211-3 (Printed version)

ISBN 978-1-74366-212-0 (HTML version)

Contents

Membership of the Committee

Chair	Mr Dan Tehan MP	
Deputy Chair	Hon Anthony Byrne MP	
Members	Mr Andrew Nikolic MP	Senator David Bushby
	Hon Tanya Plibersek MP	Senator the Hon Stephen Conroy
	Hon Philip Ruddock MP	Senator the Hon John Faulkner
	Hon Bruce Scott MP	Senator David Fawcett
		Senator the Hon Penny Wong

Terms of reference

On 16 July 2014, the National Security Legislation Amendment Bill (No. 1) 2014 was referred to the Committee by the Attorney-General.

List of abbreviations

AIC	Australian Intelligence Community
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
ASIS	Australian Secret Intelligence Service
APS	Australian Public Service
Crimes Act	*Crimes Act 1914*
Criminal Code	*Criminal Code Act 1995*
DIGO	Defence Imagery and Geospatial Organisation
IGIS	Inspector-General of Intelligence and Security
IGIS Act	*Inspector-General of Intelligence and Security Act 1986*
IS Act	*Intelligence Services Act 2001*
NSLA Bill	National Security Legislation Amendment Bill (No. 1) 2014
PID Act	*Public Interest Disclosure Act 2013*
PJCIS	Parliamentary Joint Committee on Intelligence and Security
SIO	Special Intelligence Operation

List of recommendations

3 Key issues and analysis

Recommendation 1

The Committee recommends that the Explanatory Memorandum to the National Security Legislation Amendment Bill (No. 1) 2014 be amended to clarify that the term 'ASIO affiliate' is intended to be restricted to natural persons.

Recommendation 2

The Committee recommends that the intent of proposed sections 86 and 87 contained in the National Security Legislation Amendment Bill (No. 1) 2014 be clarified to make explicit that a person on secondment shall be required to work wholly on behalf of the host organisation, and under the host organisation's legal framework.

Recommendation 3

The Committee recommends that consideration be given to amending the Explanatory Memorandum or the Attorney-General's Guidelines issued under section 8A of the *Australian Security Intelligence Organisation Act 1979* to clarify that a computer access warrant may only authorise access to a computer (which would include a network) to the extent that is necessary for the collection of intelligence in respect of a specified security matter.

Recommendation 4

The Committee recommends that the Government initiate a review of the Attorney-General's Guidelines issued under section 8A of the *Australian Security Intelligence Organisation Act 1979*, including examining requirements to govern ASIO's management and destruction of information obtained on persons who are not relevant, or no longer relevant, to security matters.

Recommendation 5

The Committee recommends that the Director-General of Security be required to include details of any instances of material disruption of a computer, or non-routine access to third party computers or premises, in the reports on the execution of each warrant provided to the Attorney-General under section 34 of the *Australian Security Intelligence Organisation Act 1979*.

Recommendation 6

The Committee recommends that the Australian Security Intelligence Organisation be required to notify the Attorney-General and the Inspector-General of Intelligence and Security within 24 hours of any incident in which force is used against a person by an ASIO officer, and for a written report on the incident to be provided within 7 days.

The Committee further recommends that the Director-General of Security be required to include details of any use of force against a person by ASIO officers in the reports on the execution of each warrant provided to the Attorney-General under section 34 of the *Australian Security Intelligence Organisation Act 1979*.

Recommendation 7

The Committee recommends that the IGIS provide close oversight of the design and execution of training for ASIO officers who may be required to use force during the execution of warrants issued under the *Australian Security Intelligence Organisation Act 1979.*

Recommendation 8

The Committee recommends that the IGIS provide close oversight of any application of the proposed powers to authorise the use of force against persons by ASIO officers to ensure those powers are used only in exceptional circumstances, and to the extent reasonable and necessary to carry out a warrant.

Recommendation 9

The Committee recommends that Schedule 3 to the National Security Legislation Amendment Bill (No. 1) 2014 be amended to require that approval must be obtained from the Attorney-General before a special intelligence operation is commenced, varied or extended beyond six months by the Australian Security Intelligence Organisation.

Recommendation 10

The Committee recommends that additional requirements be introduced into the National Security Legislation Amendment Bill (No. 1) 2014 to enhance the Inspector-General for Intelligence and Security (IGIS)'s oversight of the proposed Special Intelligence Operations scheme, including:

- a requirement for the Australian Security Intelligence Organisation (ASIO) to notify the IGIS when a special intelligence operation is approved
- a requirement for ASIO to advise the IGIS of any special intelligence operation that is intended to continue beyond six months
- a requirement for ASIO to notify the Attorney-General and the IGIS, as part of the six-monthly reports proposed in clause 35Q of the Bill, of any injury, loss or damage caused to a person or property in the course of a special intelligence operation, and
- a requirement for the IGIS to periodically, and at least annually, inspect ASIO's records relating to current special intelligence operations.

Recommendation 11

The Committee recommends that additional exemptions be included in the offence provisions relating to disclosure of information on special intelligence operations in proposed section 35P of the National Security Legislation Amendment Bill (No. 1) 2014 to explicitly enable

- disclosure of information for the purpose of obtaining legal advice
- disclosure of information by any person in the course of inspections by the Inspector-General of Intelligence and Security (IGIS), or as part of a complaint to the IGIS or other pro-active disclosure made to the IGIS
- communication of information by IGIS staff to the IGIS or other staff within the Office of the IGIS in the course of their duties.

Recommendation 12

The Committee recommends that the National Security Legislation Amendment Bill (No. 1) 2014 be amended or, if not possible, the Explanatory Memorandum of the Bill be clarified, to confirm that the Commonwealth Director of Public Prosecution must take into account the public interest, including the public interest in publication, before

initiating a prosecution for the disclosure of a special intelligence operation.

Recommendation 13

The Committee further recommends that, to make clear the limits on potential prosecution for disclosing information about special intelligence operations, Section 35P of the National Security Legislation Amendment Bill (No. 1) 2014 be amended to confirm that the mental element (or intent) of the offence is 'recklessness', as defined in the Criminal Code, by describing the application of that mental element to the specific offence created by section 35P.

Recommendation 14

The Committee recommends that the National Security Legislation Amendment Bill (No. 1) 2014 be amended to confirm that the offence provisions in Schedule 6 to the Bill do not apply to

- information disclosed to the Inspector-General of Intelligence and Security (IGIS) in the course of inspections, or in support of a complaint or other pro-active disclosure, or
- communication of information by IGIS staff to the IGIS or other staff within the Office of the IGIS in the course of their duties.

Recommendation 15

The Committee recommends that the Office of the Inspector-General of Intelligence and Security's annual budget be supplemented to the extent required to provide for the new oversight requirements associated with the National Security Legislation Amendment Bill (No. 1) 2014, including periodic reviews of special intelligence operations and oversight of the use of force during the execution of warrants.

Supplementation of the Office of the Inspector-General of Intelligence and Security's budget should also take other proposed measures to expand the powers of intelligence agencies into account.

Recommendation 16

The Committee recommends that the Government appoint an Independent National Security Legislation Monitor as soon as practicable.

Recommendation 17

The Committee recommends that, following consideration of the recommendations in this report, the National Security Legislation Amendment Bill (No. 1) 2014 be passed by the Parliament.

1

Introduction

Previous inquiry and report

1.1 In May 2012, the then Attorney-General, the Hon Nicola Roxon MP asked the Parliamentary Joint Committee on Intelligence and Security (the Committee) of the previous Parliament to inquire into a number of potential reforms to Australia's national security legislation.

1.2 The Attorney-General subsequently provided a discussion paper to the Committee outlining reforms the Australian Government was considering, as well as some on which the Government sought the views of the Committee.[1] The reforms canvassed three areas: interception of communications and access to data under the *Telecommunication (Interception and Access) Act 1979*; reform of the telecommunications security aspects of the *Telecommunications Act 1979* and other relevant legislation; and reform of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act).

1.3 The Committee's report, entitled *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, was presented to the Parliament in June 2013. The report included a total of 43 recommendations in regard

1 Attorney-General's Department, *Equipping Australia against Emerging and Evolving Threats*, July 2012.

to the possible reforms that were outlined in the discussion paper. The report is available on the Committee's website at www.aph.gov.au/pjcis.

The Bill and its referral

1.4 On 16 July 2014, the Attorney-General, Senator the Hon George Brandis QC, introduced the National Security Legislation Amendment Bill (No. 1) 2014 (the Bill) into the Senate. In his second reading speech, the Attorney-General described the Bill as a 'package of targeted reforms to modernise and improve the legislative framework governing the activities of the Australian Intelligence Community' to ensure that it 'keeps pace with the contemporary, evolving security environment'.[2]

1.5 The Attorney-General added that the Bill was 'just the first step in the Government's commitment to maintaining and, where necessary, improving Australia's already strong national security laws', noting that a 'comprehensive review of these laws' was underway that would respond to recent reviews and address any gaps identified.[3]

1.6 On the same day, the Attorney-General wrote to the Committee to refer the provisions of the Bill for inquiry and request it report by 8 September 2014. He further requested that the Committee should, as far as possible, conduct its inquiry in public.

1.7 In the letter, the Attorney-General informed the Committee that the Bill would implement the Government's response to Chapter 4 of the *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, which related to reforms to the ASIO Act and the IS Act.

Inquiry objectives and scope

1.8 The intent of the inquiry was not to debate or revisit the previous Committee's recommendations or the policy intent behind the Bill. Instead, the Committee's objectives in conducting its inquiry were to examine:

2 Senator the Hon George Brandis QC, Attorney-General, *Senate Hansard*, 16 July 2014, p. 65.

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

- whether the measures contained in the Bill appropriately implement the recommendations made by the previous Committee and the policy objectives laid out by the Government;
- whether the Bill incorporates adequate safeguards and accountability mechanisms to ensure the proper application of the laws into the future;
- whether the Bill is drafted in a way to avoid any foreseeable unintended consequences.

1.9 It is noted that at the time of this inquiry, further proposals for amendments to national security legislation were being discussed by the Government and by various commentators. These included foreshadowed legislation relating to Australians fighting in overseas conflicts and to mandatory retention of telecommunications data. These matters were not within the scope of the Committee's inquiry and are not discussed in this report.

Conduct of the inquiry

1.10 The inquiry was referred to the Committee by the Attorney-General on 16 July 2014. The Chair of the Committee, Mr Dan Tehan MP, announced the inquiry by media release on 18 July and invited submissions from interested members of the public. Following an extension, submissions were requested to be provided to the Committee by 6 August 2014.

1.11 The Committee received 30 submissions and 11 supplementary submissions from sources including government agencies, legal and civil liberties groups and members of the public. A list of submissions received by the Committee is at Appendix A. The Committee received one exhibit, which is also listed at Appendix A.

1.12 The Committee held two public hearings and two private classified hearings in Canberra on 15 August and 18 August 2014. A list of hearings and the witnesses who appeared at them is included at Appendix B.

1.13 Copies of submissions received and transcripts of public hearings can be accessed on the Committee website at www.aph.gov.au/pjcis. Links to the Bill, the Explanatory Memorandum, the report of the previous Committee and documents relating to that inquiry are also available on the Committee website.

1.14 On 4 September 2014, the Committee wrote to the Attorney-General to advise that, due to delays in the receipt of some evidence and the need to provide due scrutiny to certain issues raised, the Committee intended to report to the Parliament in the week of 22 September 2014.

Report structure

1.15 This report consists of three chapters:

- This chapter sets out the context, scope and conduct of the inquiry
- Chapter Two summarises the provisions of each of the Bill's seven schedules and considers how they relate to the previous Committee's recommendations, and
- Chapter Three contains a discussion of the main issues raised in evidence to the inquiry, and the Committee's comments and recommendations in regards to those issues.

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

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

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 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

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

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; 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]

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

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

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
>
> (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

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.

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

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]

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

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

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

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

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".
>
> 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

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.

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.

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

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.

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

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*.

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]

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.

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

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-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]

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.

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

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:

- 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

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

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

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.

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

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.

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]

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

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

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

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

'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 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

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.

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

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

> 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

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

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

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

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

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]

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:

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

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

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

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]

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:

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

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

> 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 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]

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

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.

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 '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.

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

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.

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:

> **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]

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.

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

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

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 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

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

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

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

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 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

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

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.

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 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

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

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

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

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).
- 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]

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

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

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

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 '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]

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

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

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

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.

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

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

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.

3

Key issues and analysis

Introduction

3.1 This chapter discusses the main issues raised in evidence to the inquiry, and the Committee's comments and recommendations in regard to those issues.

3.2 The intention of the chapter is not to comprehensively analyse all parts of the National Security Legislation Amendment Bill (No. 1) 2014 (the Bill) in detail, but rather to focus on the issues that were of most concern to the Committee, informed by the evidence received from inquiry participants in written submissions and at public hearings. These issues were:

- changes to the Australian Security Intelligence Organisation (ASIO) employment framework and terminology
- changes to ASIO warrant provisions, in particular relating to computer access warrants and the use of force
- the proposed Special Intelligence Operations scheme
- offences for unauthorised handling and disclosure of information, and
- oversight and scrutiny related matters.

Changes to the ASIO employment framework and terminology

ASIO affiliates

3.3 As noted in Chapter 2, the Bill includes proposals related to ASIO's employment provisions that are in addition to those examined by the Committee in its previous inquiry. In particular, as described by the Attorney-General's Department (the Department), the Bill 'consolidates the various terminology used in the *Australian Security Intelligence Organisation Act 1979* (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'.[1]

3.4 In her submission, the Inspector-General of Intelligence and Security (IGIS) noted that the proposed new concept of 'ASIO affiliate' was relevant to a number of substantive provisions in the Bill, as well as being important for the IGIS's oversight function. She noted that the definition of an 'ASIO affiliate' goes beyond employment-like relationships (such as contractors and secondees) to potentially include cleaning staff, employees of telecommunications carriers, staff of foreign government bodies, and persons providing information to ASIO.[2] At a public hearing, the IGIS explained that the boundaries of ASIO affiliate arrangements were not necessarily clear:

> [I]n terms of the fact that these people can actually exercise powers, it would be necessary, in my view, to know exactly the limits of this definition and who exactly can exercise powers.[3]

3.5 Similarly, the Law Council of Australia disagreed with the Explanatory Memorandum's characterisation of the proposed changes as 'minor or technical amendments', arguing that they '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]

3.6 Electronic Frontiers Australia indicated its concern about the broad definition of 'ASIO affiliate' in relation to cooperative intelligence operations powers:

---

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

2 Inspector-General of Intelligence and Security (IGIS), *Submission 4*, p. 6.

3 Dr Vivienne Thom, IGIS, *Committee Hansard*, Canberra, 15 August 2014, p. 1.

4 Law Council of Australia, *Submission 13*, p. 13.

> This could, as we read it, potentially extend not only to allied intelligence agencies such as the Five Eyes but also to intelligence agencies of what we might describe as uncertain virtue from any country that may be an expedient ally at any particular point in time.[5]

3.7 The Committee sought more information at hearings on the effect of the proposed amendments related to ASIO affiliates. The Attorney-General's Department explained that the term 'ASIO affiliate' was intended to consolidate a range of terms used throughout the ASIO Act and other legislation, and impose 'appropriate limitations on the scope of ASIO affiliates' authority by excluding them from being able to exercise certain powers'. The Department contended that this would not result in an expansion of the powers of non-employees, but would in fact enhance safeguards relating to their activity and provide greater certainty and clarity about their status in the legislation.[6]

3.8 ASIO's Director-General of Security explained that the biggest component of affiliates would be its 'sources', who regardless of the terminology used would still require authorisation to carry out certain activities under the Act.[7]

3.9 The Department provided more information on the intent and effect of the proposed terminology in a supplementary submission to the Committee. Responding to concerns raised by the Committee about why ASIO affiliates could be authorised to request the Australian Secret Intelligence Service (ASIS) to collect intelligence on Australian persons overseas (as provided for by Schedule 5 to the Bill, discussed below), the Department explained that this power was limited in the draft legislation to 'senior position holders'. While a 'senior position holder', as defined in Schedule 1, may include ASIO affiliates as well as ASIO employees, the term would be limited under legislation to 'an SES or equivalent level employee, or a position designated as "Coordinator". Consequently, the ability of ASIO affiliates to request cooperation from ASIS would be 'constrained to affiliates who hold senior positions within the Organisation, and who are appointed by the Director-General'.[8]

---

5 Mr Jon Lawrence, Executive Officer, Electronic Frontiers Australia, *Committee Hansard*, Canberra, 18 August 2014, p. 10.

6 Ms Jamie Lowe, Acting First Assistant Secretary, National Security Law and Policy Division, Attorney-General's Department, *Committee Hansard*, Canberra, 15 August 2014, p. 12.

7 Mr David Irvine AO, Director-General, Australian Security Intelligence Organisation (ASIO), *Committee Hansard*, Canberra, 15 August 2014, p. 13.

8 Attorney-General's Department, *Supplementary Submission 1.1*, p. 6.

3.10 In a further joint supplementary submission, the Department and ASIO responded to concerns that the use of the term 'person' in the definition of 'ASIO affiliate' could be interpreted to be applicable to 'legal persons', including foreign intelligence agencies. The submission confirmed that the use of the term 'person' was intended to be limited to natural persons. While not considering a change to the Bill to be necessary due to the applicability of the *Acts Interpretation Act 1901*, the Department and ASIO indicated that they would 'assist the Government to consider amendments to the Explanatory Memorandum to include an express statement of this intention'.[9]

Committee Comment

3.11 The Committee notes that the concept of 'ASIO affiliate' was not amongst the proposals examined in the previous Committee's inquiry into potential reforms to Australia's national security legislation. As such, the Committee was interested to explore the rationale for this inclusion in the Bill further at its hearings with the Department.

3.12 Notwithstanding the concerns raised by some inquiry participants, after seeking further clarification from the Department and the relevant agencies in both private and public hearings, the Committee was assured that the new terminology would not result in any substantial expansion to the types of persons being able to exercise or authorise the use of ASIO's powers. Any person falling into the category of 'ASIO affiliate' would still need to be delegated powers by the Director-General of Security before being able to exercise those powers. The Committee supports the intent of the provisions to consolidate the existing terminology and provide greater certainty as to the status of sources and other 'ASIO affiliates'.

3.13 While it is unlikely that the term 'ASIO affiliate' as defined in the Bill would be interpreted to include an organisation, such as a foreign intelligence organisation, the Committee considers that greater certainty on this matter is desirable. This would be achieved by putting into effect the Department and ASIO's suggestion for the intent to be made clear in the Explanatory Memorandum.

9 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 50.

Recommendation 1

The Committee recommends that the Explanatory Memorandum to the National Security Legislation Amendment Bill (No. 1) 2014 be amended to clarify that the term 'ASIO affiliate' is intended to be restricted to natural persons.

Secondment arrangements

3.14 As noted in Chapter 2, the Bill contains proposed new sections 86 and 87 to implement secondment provisions to and from ASIO, respectively, in line with a recommendation of the previous Committee.

3.15 Some inquiry participants raised concerns that there were insufficient safeguards included in the proposed sections to prevent them from potentially being misused.[10] The IGIS, for example, reiterated concerns raised in her submission to the previous inquiry that there was a need to make clear that secondments were a 'true change in working arrangements for a reasonable period' and not a 'mechanism to circumvent limits placed on employees in other legislation':

> What is not entirely clear in the Bill is whether seconded officers will retain their ASIO powers while on secondment. The Bill appears not to address this issue, though the explanatory memorandum suggests that the policy intention is that the individual will only be able to exercise the powers of the 'gaining' agency.[11]

3.16 The Law Council of Australia suggested that the relevant clauses of the Bill be modified to add a 'minimum reasonable period' for secondments, or alternatively, that this requirement be included in the Ministerial Guidelines under section 8A of the ASIO Act. The Law Council also recommended that secondment arrangements be subject to IGIS oversight, with the IGIS being required to regularly review and report on the arrangements.[12]

3.17 The Attorney-General's Department contended that the need for secondees to perform work for their host organisation, and under the legal requirements of the host organisation, was 'inherent in the nature of a

10 IGIS, *Submission 4*, pp. 6–7; Law Council of Australia, *Submission 13*, pp. 12–13; Muslim Legal Network (NSW) and Birchgrove Legal, *Submission 21*, pp. 6–7.

11 IGIS, *Submission 4*, pp. 6–7.

12 Law Council of Australia, *Submission 13*, p. 13.

"secondment", in accordance with the ordinary meaning of that term'. Further, this would be expected to be made clear in individual secondment arrangements. The Department noted, however, that an 'avoidance of doubt' styled provision could be added to Bill to clarify this intent, if it was thought desirable.[13]

Committee Comment

3.18 The Committee notes the concerns raised by the IGIS, and other inquiry participants, that the Bill does not make clear the limits within which the proposed secondment arrangements may be used. While the Committee agrees that the normal use of the term 'secondment' implies that the secondee will be working wholly for the host organisation and under the same legal framework as employees of that organisation, the Committee suggests that additional certainty would be achieved by specifying this intent in the legislation or the Explanatory Memorandum. The Committee supports the inclusion of an 'avoidance of doubt' provision to achieve this, as was proposed by the Attorney-General's Department.

Recommendation 2

The Committee recommends that the intent of proposed sections 86 and 87 contained in the National Security Legislation Amendment Bill (No. 1) 2014 be clarified to make explicit that a person on secondment shall be required to work wholly on behalf of the host organisation, and under the host organisation's legal framework.

Changes to warrant provisions

Computer access warrants

3.19 As outlined in Chapter 2, the Bill proposes to make a number of changes to the provisions for computer access warrants under the ASIO Act, including:

- amending the definition of a 'computer' to include 'one or more computer networks' (implementing, with a different choice of words, the previous Committee's Recommendation 20).

13 Attorney-General's Department, *Supplementary Submission 1.1*, p. 27; also reiterated in Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 53.

- amending the warrant provisions to allow the addition, deletion or alteration of data that either does not materially interfere with, interrupt or obstruct a communication in transit or the lawful use of a computer, or is necessary for the execution of a warrant. These proposed amendments apply to both search and computer access warrants (implementing the previous Committee's Recommendation 21).
- amending the warrant provisions to allow access to third party computers, or communications in transit, as a means to access data on a target computer; and to add, copy, alter or delete data if necessary to achieve that purpose (implementing the previous Committee's Recommendation 22).

3.20 Many submitters to the inquiry raised concerns about these elements of the proposed legislation.[14] The concerns focused on:

- The lack of definition of a 'network' in the Bill, and consequently the large number of computers, including third party computers, that could potentially be accessed under a single computer access warrant.
- The perceived low thresholds for the issue of a warrant to authorise access to third party computers. The proposed threshold stipulates that 'regard' must be given to 'any other methods of obtaining access to data', and that third party access is deemed to be 'reasonable in all the circumstances'.
- The privacy implications around how any data obtained from third party computers would be handled, and whether the private data of journalists or members of the general public could be accessed and used inappropriately.
- Lack of clarity around what constitutes a 'material' disruption of a computer that would not be permissible under the Bill's provisions.

3.21 The Committee discussed these issues further with the Attorney-General's Department and ASIO at both its public and private hearings.

---

14 Gilbert + Tobin Centre of Public Law, *Submission 2*; Dr Greg Carne, *Submission 5*; Media, Entertainment & Arts Alliance, *Submission 6*; Electronic Frontiers Australia, *Submission 9*; Law Council of Australia, *Submission 13*; Senator David Leyonhjelm, *Submission 15*; Pirate Party Australia, *Submission 18*; Councils of Civil Liberties across Australia, *Submission 20*; Muslim Legal Network (NSW) and Birchgrove Legal, *Submission 21*; Blueprint for Free Speech, *Submission 22*; Ms Alison Bevege, *Submission 23*; Dr A J Wood, *Submission 24*; Australian Interactive Media Industry Association – Digital Policy Group – Cyber Safety and Security Sub-Group, *Submission 25*; Australian Human Rights Commission, *Submission 28*.

Definition of computer network and third party access

3.22 In relation to access to third party computers, the Department explained that the new powers were necessary for ASIO to be able to circumvent the steps increasingly being taken by persons of security interest to prevent ASIO accessing their computers directly. The Department argued that only the content of the *target* computer would be accessible:

> The content of the third-party computer is not accessed under this system and could not be accessed under this system. In fact, it is of no interest to the organisation.[15]

3.23 In evidence before the Committee, representatives of the Gilbert + Tobin Centre of Public Law suggested that much of the concern around the broad definition of a computer network and access to third party computers could be mitigated by including in the Bill a definition of a 'network'. A 'minimal intrusion test', such as requiring other options for gaining the required intelligence to have been exhausted, would also ease concerns.[16]

3.24 At the Committee's request, the Centre suggested an amendment to the proposed legislation that would restrict ASIO's network access to only those parts of a network necessary for gaining information relevant to the particular investigation or person of interest.[17] The Centre's subsequent submission recommended that the following new sub-section be inserted into section 25A of the ASIO Act:

> (2A) The warrant may only authorise access to those parts of the target computer that are reasonably necessary for the collection of intelligence in respect of the security matter.[18]

3.25 In its evidence, the Department indicated that the inclusion of a 'last resort' style threshold for third party computers (similar to that applied to B-party warrants under the *Telecommunications (Interception and Access) Act 1979*) was considered to be too restrictive for ASIO's operational requirements.[19]

3.26 The Department and ASIO responded to a range of concerns and suggestions raised by other inquiry participants in relation to computer

---

15 Ms Lowe, *Committee Hansard*, Canberra, 15 August 2014, p. 14.

16 Dr Nicola McGarrity and Mr Keiran Hardy, *Committee Hansard*, Canberra, 18 August 2014, pp. 25–27.

17 Professor George Williams, *Committee Hansard*, Canberra, 18 August 2014, p. 26.

18 Gilbert + Tobin Centre of Public Law, *Supplementary Submission 2.1*, p. 2.

19 Attorney-General's Department, *Supplementary Submission 1.1*, p. 28.

access warrants in their joint supplementary submission.[20] The Department and ASIO argued that a 'minimal intrusion' test that required priority to be given to the least intrusive method of accessing data would be 'unduly restrictive'. They did not support defining a 'network' or introducing an additional issuing test in section 25A(2) of the ASIO Act, and argued that an additional 'reasonable grounds' test or additional requirements around the use of networks to access relevant data were unnecessary because of the existing limiting mechanisms in subsections 25A(2) and (4). Those subsections 'require approval of both the need to access data on a network, and the specific way in which that data is to be accessed'.[21]

3.27 In relation to third party computer access, the Department and ASIO highlighted the strength of the safeguard that such access must be 'reasonable in all of the circumstances'. The organisations emphasised that ASIO could only use a third party computer (or communication in transit) to access 'the relevant data', defined as data relevant to the 'security matter'. This would mean that data on a third party computer could not be used for any purpose other than to access data on the target computer that is relevant to the particular security matter specified in the warrant.[22]

3.28 Following private discussions with the Committee, the Department and ASIO agreed to provide advice on how the scope of the proposed new computer access powers could be narrowed to provide assurance that any access to a computer network would only be to the extent that it related to a person, entity or event of security interest. It was suggested that providing a definition of 'security matter', which any computer access is required to be related to in the current legislation, may provide the necessary assurance.[23]

3.29 In its response, the Department and ASIO pointed out that while 'security matter' was not defined in the ASIO Act (beyond that it is 'a matter that is important in relation to security'), a specific definition of 'security' was included in the Act. The submission explained that the term 'matter' was intended to take its ordinary meaning, and as such

20 Attorney-General's Department, *Supplementary Submission 1.2*, pp. 10–24.

21 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 16. It should be noted that, at the time of their submission, the Department and ASIO had not yet seen the suggested amendment provided by the Gilbert + Tobin Centre of Public Law referred to above.

22 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 23.

23 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 20.

> it is apparent that the term is capable of covering persons, entities or other things such as activities, and does not require the relevant matter to be known, in the sense that a particular person or entity, or a specific activity, must be identified. This is important because a requirement that ASIO's ability to access a computer under warrant must be linked to a known person or a known entity would significantly limit its ability to investigate serious security threats.[24]

3.30 The Department and ASIO agreed that there was a legitimate need to provide reassurance to the community in relation to what was meant by a 'security matter', and 'therefore how the thresholds for computer access would remain appropriately limited … if the proposed amendment to s 25A were enacted'. However, the submission argued that 'significant care' and 'sufficient flexibility' were required to avoid ASIO having its capability unintentionally limited.[25]

3.31 Taking these concerns into account, the Department and ASIO indicated that they considered the best way to provide reassurance on these matters to the community would be to include some commentary in the Explanatory Memorandum on the meaning of the term 'security matter' and its application to the proposed amendments. The organisations expressed their preference that, if the Committee would like such clarification to be made in legislation, this should be incorporated into the Attorney-General's Guidelines issued under the ASIO Act, rather than in the Act itself.[26]

Management of data by ASIO

3.32 Another possible issue related to the definition of 'computer' was raised in a submission from the IGIS. The IGIS noted that the proposed new definition would mean the scope of computer access warrants could be 'considerable', with implications for how the data obtained would be handled by ASIO:

> There is no obligation in the current or proposed legislation that would require ASIO at any point in time to actively consider whether information obtained under such a warrant is actually related to the individual who was the subject of the warrant and

24 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 19.

25 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 19–20.

26 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 19–20.

> no obligation to promptly delete information generated by or about individuals who are not relevant to security.[27]

3.33 Responding to the IGIS's observation in a supplementary submission, the Department agreed that section 31 of the ASIO Act 'falls short of a positive obligation on the Director-General to consider whether such records are in the possession, custody or control of the Organisation'. However, the Department noted that the propriety of ASIO's practices in this regard were 'within the IGIS's statutory remit' and suggested that operational impacts should be taken into account in any proposal to introduce such a positive obligation.[28]

3.34 Subsequent to the hearing, the IGIS wrote to suggest that the Committee consider whether an obligation should be incorporated into the legislation for ASIO to 'assess whether records are required to be retained after a period of time'. The IGIS noted that this type of obligation exists for Australian Federal Police (AFP) surveillance device warrants, for which there is a positive obligation to destroy unneeded material within five years. The IGIS also noted that such a requirement would need to be 'balanced against the resource implications for ASIO'.[29]

3.35 Related to this matter, the Office of the Australian Information Commissioner noted in its submission that, 'in view of the rapidly changing environment surrounding the data collection needs of the [Australian Intelligence Community]', it would be timely to review the Attorney-General's Guidelines for ASIO. The Guidelines currently require ASIO to

> consider the necessity and proportionality of handling personal information and, further, that any inquiries and investigations be undertaken using as little intrusion into individuals' privacy as is possible.[30]

3.36 At a public hearing, the Privacy Commissioner expanded on these comments to indicate that consideration should be given to adding into the Attorney-General's Guidelines some of the concepts that already exist in the *Privacy Act 1988* (which does not apply to ASIO), such as the

---

27 IGIS, *Submission 4*, p. 9.

28 Attorney-General's Department, *Supplementary Submission 1.1*, p. 10.

29 IGIS, *Supplementary Submission 4.1*, p. 1.

30 Office of the Australian Information Commissioner, *Submission 11*, p. 2. A copy of the current Attorney-General's Guidelines is available at http://www.asio.gov.au/About-ASIO/Oversight-and-Accountability/Attorney-General-Guidelines.html.

requirement to destroy certain information. It was noted that the Guidelines were last reviewed in 2007.[31]

3.37 In a supplementary submission, the Attorney-General's Department and ASIO acknowledged the concerns about the potential privacy impacts of the new measures in the Bill, and indicated that 'it may be timely to reconsider the Guidelines to determine if they remain appropriate in their current form or would benefit from relevant modifications'.[32]

Disruption of computers

3.38 The Department provided some clarity to the Committee, in both public and private evidence, in regard to the 'disruption' of target and third party computers. At a public hearing, the Department explained that *immaterial* interference with a computer, which would be authorised under the proposed amendments, could include 'for example, using a minor amount of storage space or bandwidth'. *Material* interference, on the other hand, would be 'extremely rare' and allowed only when necessary for the execution of a warrant.[33] The Director-General of Security elaborated that:

> We certainly could not interfere with the relevant computers such that you affected the normal and expected operation of that computer for the owner.[34]

3.39 In a supplementary submission to the inquiry, the Department further explained that the term 'material' was 'intended to take its ordinary meaning', and that the material (or otherwise) nature of any interference would be determined in individual cases and with regard to the particular circumstances. The Department noted that the legality and propriety of ASIO's activities and practices in this area would be subject to the oversight of the IGIS.[35]

3.40 In her submission, the IGIS suggested that her oversight of the new powers would be assisted if ASIO was required to provide details on any activities that interfered with or disrupted the lawful use of a computer, or

31 Mr Timothy Pilgrim, Privacy Commissioner, Office of the Australian Information Commissioner, *Committee Hansard*, Canberra, 18 August 2014, pp. 29–31.

32 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 60.

33 Ms Lowe, Attorney-General's Department, *Committee Hansard*, Canberra, 15 August 2014, p. 15.

34 Mr Irvine, ASIO, *Committee Hansard*, Canberra, 15 August 2014, p. 15.

35 Attorney-General's Department, *Supplementary Submission 1.1*, p. 9.

any access to third party computers or premises, in its reports back to the Attorney-General on the execution of each warrant.[36]

3.41 Responding to this suggestion, the Department highlighted the considerable 'administrative burden' that would result from mandating all such activities to be detailed in a report, including activities that cause non-material interference with a computer. The Department suggested the an alternative solution would be

> to distinguish between those matters considered to be sufficiently 'exceptional' to justify an indefinite, statutory reporting requirement to the Minister, and those which could be managed through practical measures (such as internal record keeping, and inspections by IGIS).[37]

Committee Comment

3.42 In reviewing the proposed amendments relating to computer access warrants, the Committee was mindful that its purpose was not to revisit the policy justifications for each of the measures, but rather to ensure the proposals contain adequate safeguards and do not give rise to unintended consequences. As such, the Committee focused its attention on exploring options to improve the clarity of the intent of the proposed measures and to ensure appropriate safeguards are in place. Balancing this is a concern not to impose impractical administrative burdens on ASIO's operations.

3.43 In relation to concerns raised about the broad interpretation of 'computer' that could result from the inclusion of the word 'network' in the definition, the Committee notes that the issue of a computer access warrant is subject to strict threshold requirements in the existing legislation. Specifically, for a warrant to be issued there needs to be 'reasonable grounds' for believing that access by ASIO to data in the specified computer will 'substantially assist the collection of intelligence … in respect of a matter (the *security matter*) that is important in relation to security'.[38] Any use of a computer that may be authorised in such a warrant is further limited in the ASIO Act to activities that are 'for the purpose of obtaining access to data that is relevant to the security matter and is held in the target computer at any time while the warrant is in force'.[39]

---

36 IGIS, *Submission 4*, p. 11.

37 Attorney-General's Department, *Supplementary Submission 1.1*, p. 28.

38 ASIO Act, subsection 25A(2).

39 ASIO Act, subsection 25A(4).

3.44 A further amendment proposed in the Bill would allow warrants to be able to authorise access to specified third party computers (and networks)—for the purpose of accessing the target data—only if it was 'reasonable in all the circumstances' with regard to any other methods of obtaining access to the data 'which are likely to be as effective'. This threshold is not as restrictive as a threshold that would require all other options to be exhausted, as some participants in the inquiry proposed. However, when taking ASIO's particular operational needs into account, this is considered by the Committee to be an appropriate safeguard to limit the scope for any potential misuse of the third party access warrants.

3.45 The proposed third party access provisions do not allow ASIO to access a third party computer for any purpose other than to obtain access to data on the target computer. The Committee considers that the proposed amendment would therefore be more accurately described as enabling third party computers (or networks) to be used as a *conduit* to the target computer, rather than enabling access to content on the third party computer.

3.46 The Committee notes that an explicit requirement in the warrant provisions regarding the scope and purpose of computer access—along the lines suggested by the Gilbert + Tobin Centre of Public Law—could provide a useful additional safeguard to remove any doubt about the potential for the powers to be used beyond the scope intended. Nonetheless, the Committee is conscious of the need to avoid any unintended restrictions on ASIO's ability to access the information it needs to operate most effectively.

3.47 The Committee accepts the Department and ASIO's argument that the existing safeguards in the legislation are sufficient to limit ASIO's access to networks to specific security matters. The Committee endorses the proposal of the Department and ASIO for greater clarity with regard to these matters in the Bill's Explanatory Memorandum and/or the Attorney-General's Guidelines.

Recommendation 3

The Committee recommends that consideration be given to amending the Explanatory Memorandum or the Attorney-General's Guidelines issued under section 8A of the *Australian Security Intelligence Organisation Act 1979* to clarify that a computer access warrant may only authorise access to a computer (which would include a network) to the extent that is necessary for the collection of intelligence in respect of a specified security matter.

3.48 The Committee recognises that the provisions relating to computer access warrants will provide ASIO with important tools to keep abreast of technological advances that were not envisaged when the ASIO Act was originally drafted. However, there is also a need for ASIO to ensure its expanded capabilities to gather information from digital sources are balanced with safeguards to ensure that such information, as it relates to persons not of security interest, is handled in an appropriate manner. While the Committee does not doubt the propriety of ASIO's current internal procedures in this area, it considers that steps to formalise good practice in respect to this information would help provide public assurance of this propriety into the future.

3.49 The Committee recognises the considerable administrative burden that a positive obligation for the review and destruction of records could place onto ASIO if not framed carefully. While the Committee does not consider that a desire for administrative efficiency should outweigh the protection of individuals' privacy, it hesitates to recommend that restrictive requirements in this area be enshrined in the ASIO Act. As a more flexible alternative to creating a statutory requirement for ASIO to continuously review the information it holds, the Committee supports the Privacy Commissioner's suggestion for a review of the Attorney-General's Guidelines to update its privacy provisions. Such a review would need to take into account both privacy concerns and the unique requirements of ASIO's operational model.

3.50 The Committee considers that such a review would be timely given the rapidly changing technologies being employed by both ASIO and its targets. In the absence of any specific concerns about ASIO's current practice, the conduct of such a review is not considered urgent and should not delay the passage of the Bill under consideration. Nonetheless, the Committee recommends that a review of the Guidelines be initiated.

Recommendation 4

The Committee recommends that the Government initiate a review of the Attorney-General's Guidelines issued under section 8A of the *Australian Security Intelligence Organisation Act 1979*, including examining requirements to govern ASIO's management and destruction of information obtained on persons who are not relevant, or no longer relevant, to security matters.

3.51 The Committee was satisfied with the Department and ASIO's clarifications, both in public and private hearings, about what would be considered material disruption or interference with a computer. The Committee agrees that good record keeping by ASIO in regard to its activities in this area will be essential for supporting adequate oversight by the IGIS.

3.52 The Committee supports the IGIS's suggestion for reports on the execution of warrants provided to the Attorney-General to include details of computer interference, as well as any third party access. In order to avoid these reports becoming an unnecessary administrative burden on ASIO, the Committee agrees with the Department's proposal for such reporting to be limited to exceptional activities. The Committee suggests that the category of 'exceptional' would constitute any *material* disruption of a computer (noting that the Committee has been assured this power is intended to be used only rarely), as well as any non-routine access to third party computers or premises.

Recommendation 5

The Committee recommends that the Director-General of Security be required to include details of any instances of material disruption of a computer, or non-routine access to third party computers or premises, in the reports on the execution of each warrant provided to the Attorney-General under section 34 of the *Australian Security Intelligence Organisation Act 1979*.

Use of force against a person

3.53 As noted in Chapter 2, the previous Committee recommended that the use of force *against a person* should be excluded from any proposed provisions to clarify the permissible use of force in the execution of a warrant. The Government did not agree with this recommendation and, as such, the

proposed amendments in the Bill would authorise the use of 'reasonable force' against both 'persons and things'.

3.54 At a public hearing, the Committee sought clarification with ASIO and the Attorney-General's Department as to the intent and rationale behind this decision. The Director-General of Security explained that, in most cases, the use of force attached to the execution of an ASIO Act warrant would be carried out by law enforcement officers from the Australian Federal Police (AFP), who often assist ASIO in the execution of warrants. Those law enforcement officers were dependent on the use of force being permissible under the ASIO Act:

> At the moment, we as ASIO officers cannot use force, but nor can the AFP because it is under an ASIO warrant and not a law enforcement warrant … if that power were granted under an ASIO warrant it would still be the properly trained and qualified police officers who would carry out that physical activity.[40]

3.55 The Director-General further explained that there would be some occasions, due to a 'particular level of sensitivity', in which it would not be appropriate for law enforcement officers to be present during the execution of a warrant. In these instances, ASIO officers may be required to exercise force, and special training would need to be provided for ASIO officers involved in such operations.[41]

3.56 In her submission to the Committee, the IGIS also highlighted the need for appropriate training to be provided to any ASIO officers that may be required to use force against a person. The IGIS added that 'proper oversight' of such use of force would 'require oversight of the training program as well as prompt reporting and review of any instance where an ASIO employee or ASIO affiliate used force against a person'.[42] At the public hearing the IGIS elaborated that the training would require 'quite a lot of diligence', and her oversight would comprise the following:

> We would not be physically present at the training … but we would look at the training that they recommend and we might, for example, compare it to the AFP's training regime.[43]

---

40 Mr Irvine, ASIO, *Committee Hansard*, Canberra, 15 August 2014, p. 17. Other evidence from the Attorney-General's Department and ASIO indicated that it was not currently clear in the Act whether the use of force against persons was permissible.

41 Mr Irvine, ASIO, *Committee Hansard*, Canberra, 15 August 2014, pp. 17–18.

42 IGIS, *Submission 4*, p. 13.

43 Dr Thom, IGIS, *Committee Hansard*, Canberra, 15 August 2014, p. 4.

3.57 The IGIS's submission also indicated that it would assist her oversight if the Attorney-General and the IGIS were 'notified as soon as possible if, in the execution of *any* ASIO warrant, force was used against a person'.[44]

Committee comment

3.58 As noted above, the previous Committee recommended in its 2013 inquiry that any amendment to the ASIO Act to explicitly authorise the use of force during the execution of a warrant should make clear that this force is to be used only against property, and not persons. The current Committee continues to hold a firm view that any use of force against a person during the execution of a warrant would be the proper role of law enforcement agencies, not ASIO officers.

3.59 The Committee accepts the need to clarify in the legislation that force may be used by law enforcement officers assisting ASIO during the execution of a warrant. ASIO must take all steps possible to ensure that law enforcement officers are available for this purpose.

3.60 However, following evidence presented during this inquiry, the Committee understands that there may be rare circumstances in which, due to a particular level of sensitivity, ASIO would not be accompanied by law enforcement officers during the execution of a warrant. It also understands there may be extremely rare occasions when it is not physically possible, due to the urgency of a situation, for law enforcement officers to be present. The Committee considers that these occasions should be strictly limited to exceptional circumstances in which it is operationally essential that police not be involved or in which, due to an emergency situation, it is operationally impractical for them to be.

3.61 The Committee believes that any use of force against a person by ASIO officers should be extremely rare, and must not become a normal part of operations. If not appropriately constrained, the use of force against persons by ASIO officers could, over time, change the basic premise of the way ASIO operates.

3.62 The Committee endorses the view of the IGIS that the design and execution of training in the use of force—for the limited number of ASIO officers who may need to use it—will be vitally important, and encourages the IGIS to pay close attention to the design of this training, particularly in its early stages.

44 IGIS, *Submission 4*, p. 14.

3.63 The Committee is constrained under section 29 of the *Intelligence Services Act 2001* in its ability to investigate operational matters and therefore to monitor the use of force against persons by ASIO officers and to ensure the proposed powers are used on an exceptional basis only. If these powers are used, the Committee believes it is essential that the IGIS ensure they are properly applied. The Committee makes the following recommendations to assist the IGIS in her oversight:

Recommendation 6

The Committee recommends that the Australian Security Intelligence Organisation be required to notify the Attorney-General and the Inspector-General of Intelligence and Security within 24 hours of any incident in which force is used against a person by an ASIO officer, and for a written report on the incident to be provided within 7 days.

The Committee further recommends that the Director-General of Security be required to include details of any use of force against a person by ASIO officers in the reports on the execution of each warrant provided to the Attorney-General under section 34 of the *Australian Security Intelligence Organisation Act 1979*.

Recommendation 7

The Committee recommends that the Inspector-General of Intelligence and Security provide close oversight of the design and execution of training for ASIO officers who may be required to use force during the execution of warrants issued under the *Australian Security Intelligence Organisation Act 1979*.

Recommendation 8

The Committee recommends that the Inspector-General of Intelligence and Security provide close oversight of any application of the proposed powers to authorise the use of force against persons by ASIO officers to ensure those powers are used only in exceptional circumstances, and to the extent reasonable and necessary to carry out a warrant.

Special Intelligence Operations scheme

3.64 Many inquiry participants raised concerns in their evidence to the Committee about aspects of the proposed Special Intelligence Operations (SIO) scheme outlined in Schedule 3 to the Bill.[45] The main concerns raised can be summarised as relating to:

- the rationale for a special intelligence operations scheme that provides immunity to its participants
- the few limitations on the types of conduct that could be authorised under an SIO
- the relative lack of safeguards when compared to the 'controlled operations' regime in the *Crimes Act 1914* (the Crimes Act), which applies to law enforcement agencies, including:
  - ⇒ that individual SIOs are proposed to be approved internally, rather than through an independent authority
  - ⇒ the apparently lower threshold test for new SIOs
  - ⇒ the longer duration of SIO authorisations
  - ⇒ less comprehensive oversight mechanisms
  - ⇒ less detailed reporting and record keeping requirements, and
  - ⇒ a lack of provisions for compensation in respect of any harm done

45 Gibert + Tobin Centre of Public Law, *Submission 2*; Mr Bill Calcutt, *Submission 3*; Media, Entertainment & Arts Alliance, *Submission 6*; Australian Lawyers Alliance, *Submission 7*; Electronic Frontiers Australia, *Submission 9*; Guardian Australia, *Submission 12*; Law Council of Australia, *Submission 13*; Senator David Leyonhjelm, *Submission 15*; Joint media organisations, *Submission* 17; Professor A J Brown, *Submission* 19; Civil Liberties Councils across Australia, *Submission 20*; Muslim Legal Network and Birchgrove Legal, *Submission 21*; Blueprint for Free Speech, *Submission 22*; Ms Alison Bevege, *Submission 23*; Australian Human Rights Commission, *Submission 28*.

- the offence provisions under proposed section 35P for disclosing any information on an SIO, including:
  - ⇒ the broad scope of the basic, non-aggravated offence, including its applicability to journalists, lawyers and whistle-blowers
  - ⇒ the necessity of having specific offences for SIOs
  - ⇒ the severity of the maximum penalties for the offences
  - ⇒ the lack of a public interest defence or other whistle-blower protections, and
  - ⇒ the potential for the offences to have a 'chilling effect' on public debate on national security matters, media reporting and whistle-blowing; and
- the desirability of a mandatory review of the scheme after a certain period, accompanied by a sunset clause in the legislation.

3.65 The Committee followed up many of these concerns with the Attorney-General's Department and ASIO at its public and private hearings. At a public hearing, the Department highlighted the 'very specific safeguards' in the legislation that would prevent SIO arrangements from being 'used in bad faith or for an ulterior purpose':

> [A] special intelligence operation cannot be authorised unless the authorising officer is satisfied on reasonable grounds that such an operation would assist the organisation in the performance of a special intelligence function … The authorising officer must also be satisfied on reasonable grounds that the circumstances are such as to justify a special intelligence operation. There must be a written record of that authorisation, documenting how the operation will assist the organisation in the performance of one or more of its functions. There is also a requirement that ASIO submit six-monthly reports to the Attorney-General and the IGIS explaining how the operation has in fact assisted the organisation in the performance of its functions.[46]

3.66 The Department and ASIO addressed many of the concerns raised by inquiry participants in their supplementary submissions.[47] Further detail on specific issues that were focused on during the inquiry is summarised below.

---

46 Ms Lowe, Attorney-General's Department, *Committee Hansard*, Canberra, 15 August 2014, p. 12.

47 Attorney-General's Department, *Supplementary Submission 1.1*; Attorney-General's Department and ASIO, *Supplementary Submission 1.2*.

Authorisation of SIOs

3.67 The Committee considered the question of whether new SIOs should be authorised internally by the Director-General of Security (or his deputies) as currently proposed in the Bill, or through an external, independent authority.

3.68 In a submission to the inquiry, the Department discussed provisions in the Crimes Act that provide for independent, external authorisation of controlled operations that extend beyond three months. The Department explained that these provisions were not replicated in the proposed SIO scheme due to the 'separate purposes to which each scheme is directed'. A particular difference highlighted was that intelligence operations were often longer term than controlled operations and were aimed at gathering intelligence over a period of time. The Department indicated that the Director-General of Security and his deputies were the best placed to make decisions, including in 'time critical circumstances', about the commencement and conduct of SIOs as they have the 'necessary visibility and detailed understanding of the security environment and the conduct of intelligence operations'.[48]

3.69 Noting that submitters to the inquiry had expressed concern about the proposal for SIOs to be authorised internally, the Committee asked other participants in the public hearings whether a requirement to gain authorisation from an external, independent issuing authority would help to allay their concerns about the scheme. All of those asked indicated that this would be a positive step.[49]

3.70 After the Committee sought further input on the practical aspects of introducing an independent issuing authority for SIOs, the Department and ASIO indicated their strong preference for an internal authorisation process to be retained. The organisations expanded on their contention that decisions about the commencement, continuation and conduct of SIOs required 'an extensive awareness and sophisticated understanding of the security environment' as well as a 'strong practical understanding of the way in which intelligence operations are conducted'. It was argued that such expertise was 'essential' for making decisions about SIOs 'in time critical and rapidly developing circumstances'.[50]

48 Attorney-General's Department, *Supplementary Submission 1.1*, p. 25.

49 Mr Stephen Keim SC, Law Council of Australia, *Committee Hansard*, Canberra, 18 August 2014, p. 7; Dr Lesley Lynch, NSW Council for Civil Liberties, *Committee Hansard*, Canberra, 18 August 2014, p. 17; Professor Williams, Gilbert + Tobin Centre of Public Law, *Committee Hansard*, Canberra, 18 August 2014, p. 24.

50 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 26.

3.71 The Department and ASIO were further concerned that any move to an external authorisation model would 'transfer primary decision making on a core operational matter to a person who is not responsible for the Organisation's performance' and who 'lacks the requisite understanding of the security environment and operational expertise'. The organisations argued that appointing multiple external issuing authorities could also risk inconsistency in decision-making, and that such an external authorisation model could reduce the scope for the IGIS to conduct oversight of authorisation decisions.[51]

3.72 For similar reasons, the Department and ASIO also argued against a model of authorisation by the Attorney-General. The organisations noted that this alternative would have 'fewer adverse operational impacts than decision making by an external issuing authority' as a consequence of the Attorney-General's overall responsibility for security matters and 'broad awareness of the security environment'. The Department and ASIO indicated that their concerns about the 'necessary degree of operational background and expertise to make authorisation decisions' would also apply to this proposal, although 'to a lesser extent'. They argued that the authorisation of an SIO would be an inherently different decision to the approval of an ASIO warrant, which currently requires the Attorney-General's approval.[52]

3.73 Acknowledging the concerns of the Committee and inquiry participants, the Department and ASIO proposed an alternative solution in which additional notification requirements would be built into the scheme in order to improve oversight by the Attorney-General and the IGIS. Specifically, the following requirements were proposed:

- A new requirement to notify the IGIS when a special intelligence operation authority is granted, to provide the IGIS with the opportunity to conduct effective oversight from the commencement of any operation.
- A new requirement that ASIO advise the Attorney-General and the IGIS of any special intelligence operation where there is an intention for that operation to continue beyond six months. This would enable both the Attorney-General and the IGIS to raise any concerns, and to make decisions about the level of scrutiny to which it will be subject.
- An additional notification requirement in proposed s 35Q, requiring the Director-General to inform the Attorney-General and the IGIS, as part of six monthly reporting on operations, if

51 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 26–28.

52 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 29.

any injury, loss or damage was caused to a person or property in the course of, or as a result of, the operation. This would enable the IGIS to undertake any relevant inquiries, and to consider making recommendations as to the payment of compensation as appropriate.

- If the Committee requires statutory assurance that oversight powers will be exercised in relation to special intelligence operations (in addition to the general oversight powers of the IGIS) a similar provision to s 15HS of the Crimes Act could potentially be included (relating to inspection of controlled operation records) requiring the IGIS to periodically inspect records relating to current special intelligence operations (for example, annually).[53]

3.74 The Department and ASIO additionally suggested that 'further assurance of accountability and oversight' could be provided by limiting the power to approve an SIO to the Director-General of Security alone. This power is currently proposed to be also invested in the Deputy Director-Generals.[54]

Reporting and record-keeping

3.75 In her submission to the inquiry, the IGIS noted that 'periodic review during the life of the operation, not only at its conclusion' would be necessary given the potential for SIOs to run over many years. The IGIS added that the reporting obligations for SIOs proposed in the Bill were limited to 'the extent to which the special intelligence operation has assisted ASIO in the performance of one or more of its special intelligence functions' and 'basic statistical information'. Good record keeping on the part of ASIO, it was argued, would therefore be essential to enable the IGIS's effective oversight of the SIOs.[55]

3.76 Appearing before the Committee, the Assistant IGIS elaborated that the Bill's proposal for six-monthly reporting on the extent to which the SIO assisted ASIO would not be useful for the purpose of oversight:

> It is not whether it assisted ASIO; it is more whether the conduct under that operation has been appropriate, proportionate and reasonable and what actually has gone on. So the current reporting requirement would not be the information we would need; we would need a lot more. If there is no express reporting

53 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 30.

54 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 30.

55 IGIS, *Submission 4*, p. 15.

> requirement, we would rely heavily on ASIO's ability to keep appropriate records.[56]

3.77 In discussions with the Committee, other participants also indicated their support for the IGIS to have oversight of SIOs as they occurred, not just after they had concluded.[57]

3.78 Responding to the IGIS's submission, the Department acknowledged the suggestion that 'contemporaneous report (such as on the commencement of an operation) could assist in conducting oversight'. However, the Department cautioned that consideration of an additional statutory requirement for such reporting would 'need to be weighed carefully against potential operational impacts'.[58]

3.79 In a further supplementary submission, the Department and ASIO explained that a detailed regime for reports to the IGIS, similar to that in the Crimes Act for reports on controlled operations to the Ombudsman, was not necessary because, unlike controlled operations, SIOs would only involve participants associated with a single agency (ASIO). The Departments highlighted that the IGIS's ability to conduct oversight over the SIO scheme would be enhanced by the proposal for increased notification requirements discussed above.[59]

SIO offence provisions

3.80 Many of the concerns about the SIO scheme raised by participants in the inquiry related to the offence provisions under proposed section 35P. In particular, concerns were raised that a well-intentioned person, such as a journalist, who disclosed information about an SIO which that person considered to be in the public interest, may face the possibility of prosecution under the basic, non-aggravated offence carrying a five-year maximum term of imprisonment. Concern was also raised that such a prosecution could take place even if the person was not aware that the disclosed information related to an SIO. The Committee explored these issues at length in its discussions with the Attorney-General's Department.

---

56 Mr Jake Blight, Office of the Inspector General for Intelligence and Security, *Committee Hansard*, Canberra, 15 August 2014, p. 6.

57 Mr Keim, Law Council of Australia, *Committee Hansard*, Canberra, 18 August 2014, p. 7; Professor Williams, Gilbert + Tobin Centre of Public Law, *Committee Hansard*, Canberra, 18 August 2014, p. 24.

58 Attorney-General's Department, *Supplementary Submission 1.1*, p. 29.

59 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 40–41.

3.81 The Department provided detailed advice on the reasons behind the design of the offences in the SIO scheme in a submission to the Committee. The submission included the Department's view on why the existing (and proposed) offences relating to unauthorised disclosure of information in other parts of the ASIO Act, the *Criminal Code Act 1995* (the Criminal Code) and the Crimes Act, would not adequately cover the proposed SIO scheme. The Department argued that although an offence in section 79(3) of the Crimes Act could apply to the same conduct that was being targeted by the new non-aggravated offence in proposed section 35P, the maximum sentence for that offence was 'disproportionally low' for a covert intelligence operation:

> A maximum penalty of two years' [imprisonment] would not provide a sentencing court with an adequate range within which to impose a sentence that reflects the gravity of the consequences of the conduct constituting the offence. As such, a two-year sentence … would be unlikely to serve as a significant deterrent to persons who may be contemplating communicating information relating to a special intelligence operation.[60]

3.82 At the public hearing, the Department explained that the offence provisions were 'intentionally designed' not to cover journalists reporting on an activity unaware that it was an SIO. It pointed out that the prosecution would be required to prove that a person who communicated information on an SIO was 'reckless as to the possibility that the information related to [an SIO]'. This was a result of the application of the Criminal Code's 'fault element of recklessness', which

> requires proof beyond reasonable doubt of two matters: firstly, that the person was aware of a substantial risk that the information related specifically to [an SIO] and, secondly, that the person nonetheless and unjustifiably in the circumstances took that risk of communicating the information.[61]

3.83 The Department argued that the fault element of recklessness was 'not a low threshold by any means', and that 'there would be difficulty in inadvertently or accidentally crossing that threshold'.[62] The Department's supplementary submission elaborated on this point in detail:

---

60 Attorney-General's Department, *Supplementary Submission 1.1*, pp. 16–17.

61 Ms Lowe, Attorney-General's Department, *Committee Hansard*, Canberra, 15 August 2014, p. 10.

62 Ms Lowe, Attorney-General's Department, *Committee Hansard*, Canberra, 15 August 2014, p. 20.

> [A] successful prosecution could not be brought against a person who disclosed information without any awareness that it could relate to [an SIO], since there would be no evidence of an advertence to a risk of any kind … The Department does not accept suggestions that a mere awareness that ASIO is, or may be, involved in an activity of any kind must necessarily give rise to awareness of a substantial risk that there was a special intelligence operation on foot, particularly given the criminal standard of proof that would apply. Any awareness of substantial risk must also be considered alongside the second component of the fault element of recklessness, that taking that risk (making the disclosure) was unjustifiable in the circumstances known to the person at the time.[63]

3.84 The Department also noted that there were comparable offences in the Crimes Act relating to AFP controlled operations, for which no issues had been raised to date.[64] The Department's submission further pointed out that, as with police controlled operations, journalists would have the opportunity to contact ASIO for guidance and clarification when needed:

> [A]dvice from law enforcement agencies is that media professionals have engaged effectively with them in seeking guidance or clarification about reporting on such matters, in order to avoid the risk of unintentionally compromising sensitive operations. Media professionals can similarly contact [ASIO] on a publicly listed telephone number on the Organisation's website. The media telephone line is staffed 24 hours.[65]

3.85 The Department made the following additional points about the safeguards in the proposed offence provisions in its supplementary submission:

- An exception is included in the proposed section 35P(3) of the Bill for disclosures made for the purposes of any legal proceedings related to the SIO scheme, and the reporting of those proceedings.
- It would not be appropriate to include a specific exemption from the offence provisions for journalists, as non-disclosure obligations should apply equally to all members of the community.

---

63 Attorney-General's Department, *Supplementary Submission 1.1*, p. 21.

64 Ms Lowe, Attorney-General's Department, *Committee Hansard*, Canberra, 15 August 2014, p. 10.

65 Attorney-General's Department, *Supplementary Submission 1.1*, p. 17.

- Unlike in the Crimes Act provisions for AFP controlled operations, the proposed SIO offence provisions do not contain an 'express defence for good faith disclosure of information to an independent oversight body'. This was because the relevant provisions in the Crime Act pre-date the *Public Interest Disclosure Act 2013*, which allows suspected wrongdoing in relation to SIOs to be disclosed to the Director-General of Security and the IGIS.
- The Commonwealth Director of Public Prosecutions has discretion in regard to whether to commence a prosecution, and as part of making that decision is required to consider whether a potential prosecution is in the public interest.[66]

3.86 Following a request from the Committee in a private hearing, the Department and ASIO provided a further supplementary submission which considered the differences in accountability requirements between the proposed SIO scheme and the existing controlled operations scheme in the Crimes Act.[67]

3.87 In relation to the proposed offence provisions, the Department and ASIO noted that it had not considered it necessary to replicate in the SIO scheme's offences an exception for disclosure of information for the purpose of obtaining legal advice, as exists in the Crimes Act. However, the submission noted concerns raised during the inquiry that persons who are not participants in an SIO scheme may be exposed to liability in the course of seeking legal advice related to a SIO.[68] The Department and ASIO indicated that a further exemption could be added for legal advice, in addition to the existing proposed exemption in relation to legal proceedings:

> This could provide a greater degree of reassurance to persons who may wish to consult a lawyer to better understand any legal rights or obligations that may apply to them, but not necessarily for the purpose of commencing legal proceedings.[69]

3.88 The Department and ASIO also indicated in their submission that another exemption could be added in regard to the disclosure of information on an SIO to the IGIS. The submission noted that 'such an exemption was not considered necessary' because of the immunities offered in the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act), the *Public Interest*

66 Attorney-General's Department, *Supplementary Submission 1.1*, pp. 22–24.

67 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 31–48, 86–96.

68 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 42.

69 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 47.

Disclosure Act 2013 (PID Act), and the 'exercise of prosecutorial discretion'. However, after considering the IGIS's evidence to the inquiry (discussed below in relation the offences in Schedule 6 to the Bill), the Department and ASIO acknowledged that 'an express exception would be desirable to provide certainty that disclosures to the IGIS are not subject to the offences'. Specifically, it was suggested that this exception should cover disclosures made to the IGIS by 'persons other than public officials for the purpose of the PID Act' and 'disclosures made by staff of the IGIS to the IGIS or other staff members in that Office for the purpose of performing inspection (as distinct from inquiry) functions under the IGIS Act.[70]

Committee comment

3.89 After considering the matter in its 2013 inquiry, the Committee previously recommended that a controlled intelligence operation scheme be introduced 'subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime'. The purpose of this current inquiry is not to reconsider the rationale for such a scheme, but rather to assess the adequacy of the safeguards included in the scheme as it is proposed, including its offence provisions. The Committee notes that, despite its previous recommendation being 'supported',[71] not all the safeguards included in the AFP controlled operations regime are included in the SIO scheme proposed in this Bill.

3.90 During the inquiry, the Committee suggested that many of the concerns raised by participants about the potential for misuse, or overuse, of the SIO scheme would be allayed if an independent issuing authority was required to authorise the commencement of any new SIO. The purpose of such a model would be to lessen the perceived risk of SIO powers being used for purposes beyond those envisaged in the Bill, and through this, strengthening public confidence in the integrity of the scheme.

3.91 Nonetheless, the Committee is conscious that any alternative authorisation model should not impede ASIO's operational requirements to initiate SIOs in a timely and considered manner. The Committee accepts the Attorney-General's Department and ASIO's reservations that an external authorisation model may impede timely and effective operations.

3.92 The Committee considers that the alternative proposal by the Department and ASIO for additional requirements around notifications and reporting would significantly enhance the IGIS's (and Attorney-General's) oversight

70 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 42.

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

of the SIO regime. In particular, the proposals would enhance the ability of the IGIS to oversee the commencement of new SIOs and to assess any potential need for compensation due to injury, loss or damage to persons or property.

3.93 The Committee also considers that the suggested requirement for the IGIS to periodically inspect the records of current SIOs would be effective in encouraging sustained, close scrutiny of the scheme's operation into the future. The Committee encourages the IGIS to pay particularly close attention to decisions to authorise the commencement or variation of each SIO to ensure their ongoing compatibility with the stated intent of the scheme.

3.94 While these proposals are helpful and will strengthen oversight of the SIO regime by the IGIS, the Committee is not convinced that retrospective oversight is sufficient given the seriousness of action that could be taken under an SIO and the necessary lack of public transparency over those actions. The Committee considers that an additional level of authorisation should be required to be obtained by ASIO before an SIO can commence. Taking into account concerns about the operational impact of an external authorisation regime, and also the need for sufficient oversight and accountability, the Committee is of the view that authorising approval from the Attorney-General should be a requirement of an SIO.

3.95 The Committee therefore makes the following two recommendations to strengthen the integrity of oversight requirements for the SIO scheme:

Recommendation 9

The Committee recommends that Schedule 3 to the National Security Legislation Amendment Bill (No. 1) 2014 be amended to require that approval must be obtained from the Attorney-General before a special intelligence operation is commenced, varied or extended beyond six months by the Australian Security Intelligence Organisation.

Recommendation 10

The Committee recommends that additional requirements be introduced into the National Security Legislation Amendment Bill (No. 1) 2014 to enhance the Inspector-General for Intelligence and Security (IGIS)'s oversight of the proposed Special Intelligence Operations scheme, including:

- **a requirement for the Australian Security Intelligence Organisation (ASIO) to notify the IGIS when a special intelligence operation is approved**
- **a requirement for ASIO to advise the IGIS of any special intelligence operation that is intended to continue beyond six months**
- **a requirement for ASIO to notify the Attorney-General and the IGIS, as part of the six-monthly reports proposed in clause 35Q of the Bill, of any injury, loss or damage caused to a person or property in the course of a special intelligence operation, and**
- **a requirement for the IGIS to periodically, and at least annually, inspect ASIO's records relating to current special intelligence operations.**

3.96 As SIOs are expected to be used only in the most highly sensitive circumstances, the Committee accepts the need for specific offence provisions to confer a higher level of protection for information about SIOs than for other operational matters. The Committee notes that the specific offence provisions contained in proposed section 35P of the Bill were modelled on similar provisions contained in the *Crimes Act 1914* for law enforcement controlled operations.

3.97 The Committee appreciates the Department's efforts to directly and comprehensively respond to concerns raised by inquiry participants about the offence provisions in the proposed SIO scheme.[72]

3.98 The Committee paid close attention to concerns raised by inquiry participants about the potential impact of the proposed offences on press freedom. The Committee considers that in order to ensure the success of highly sensitive operations and to protect the identity of individuals involved, it is essential that information on these operations not be disclosed.

72 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*.

3.99 However, the Committee also considers that it is important for this need for secrecy not to penalise legitimate public reporting. The Committee notes that, under the *Criminal Code Act 1995*, the fault element of 'recklessness' would apply to any prosecution of offences under proposed section 35P. This would mean that to be successful, the prosecution would be required by legislation to prove that a disclosure was 'reckless'. The structure of the offence provisions, as well as the requirement for the Commonwealth Director of Public Prosecutions to take the public interest into account before initiating a prosecution, provides an appropriate level of protection for press freedoms while balancing national security. However the Committee sees value in making these safeguards explicit in the Bill or the Explanatory Memorandum.

3.100 The Committee considers that these safeguards, coupled with increased oversight by the IGIS over the issuing of SIOs, will provide appropriate protection for individuals, including journalists, who inadvertently make a disclosure of information about a current SIO. The Committee also highlights the important role of ASIO's existing 24-hour media unit in providing opportunities for journalists to clarify any concerns about a possible operation, including about the re-publication of any information.

3.101 Taking these safeguards into account, the Committee does not consider it appropriate to provide an explicit exemption for journalists from the proposed offence provisions. Part of the reason for this is that the term 'journalism' is increasingly difficult to define as digital technologies have made the publication of material easier.[73] The Committee considers that it would be all too easy for an individual, calling themselves a 'journalist', to publish material on a social media page or website that had serious consequences for a sensitive intelligence operation. It is important for the individual who made such a disclosure to be subject to the same laws as any other individual.

3.102 The Committee is, however, concerned to ensure that any unintended consequences of the proposed SIO offence provisions are avoided. As such, the Committee fully supports the Department and ASIO's suggestion to introduce an explicit exemption from the offences for disclosure of information in the course of obtaining legal advice.

3.103 The Committee also supports explicit exemptions to be introduced for the disclosure of information to the IGIS. To avoid any doubt about the

73 The difficulty with defining 'journalism' was discussed with the Media, Entertainment & Arts Alliance at a public hearing. See *Committee Hansard*, Canberra, 18 August 2014, pp. 34–35.

applicability of the PID Act,[74] the Committee considers it should be made explicit in the Bill that this exemption applies to all persons making a complaint to the IGIS, including public officials.

Recommendation 11

The Committee recommends that additional exemptions be included in the offence provisions relating to disclosure of information on special intelligence operations in proposed section 35P of the National Security Legislation Amendment Bill (No. 1) 2014 to explicitly enable

- **disclosure of information for the purpose of obtaining legal advice**
- **disclosure of information by any person in the course of inspections by the Inspector-General of Intelligence and Security (IGIS), or as part of a complaint to the IGIS or other pro-active disclosure made to the IGIS**
- **communication of information by IGIS staff to the IGIS or other staff within the Office of the IGIS in the course of their duties.**

Recommendation 12

The Committee recommends that the National Security Legislation Amendment Bill (No. 1) 2014 be amended or, if not possible, the Explanatory Memorandum of the Bill be clarified, to confirm that the Commonwealth Director of Public Prosecution must take into account the public interest, including the public interest in publication, before initiating a prosecution for the disclosure of a special intelligence operation.

74 For the same reasons as discussed below in regard to the offence provisions in Schedule 6 to the Bill, acknowledged by the Department and ASIO. See IGIS, *Submission 4*, p. 20 and Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, p. 49.

Recommendation 13

The Committee further recommends that, to make clear the limits on potential prosecution for disclosing information about special intelligence operations, Section 35P of the National Security Legislation Amendment Bill (No. 1) 2014 be amended to confirm that the mental element (or intent) of the offence is 'recklessness', as defined in the Criminal Code, by describing the application of that mental element to the specific offence created by section 35P.

Offences for unauthorised handling and communication of information

3.104 In addition to the specific unauthorised disclosure offences relating to the SIO scheme, many inquiry participants raised broader concerns about the increased penalties and new offences for unauthorised disclosure and handling of information proposed in Schedule 6 to the Bill.[75] The main concerns raised were that:

- the proposed penalties for the existing and new offences are excessive compared to similar provisions in other legislation, including the Crimes Act
- the existing and proposed new offences do not require an *intent* to harm national security, for national security to *in fact* be harmed, or for the information involved to be *relevant* to national security
- no defence is provided in relation to disclosure of information that is already in the public domain, if the Commonwealth has not given its authority to release the information
- under the *Public Interest Disclosure Act 2013* (PID Act), there is inadequate protection from the existing and proposed new offences for whistle-blowers in intelligence agencies, and
- there is no need for the proposed new offences because the conduct they seek to punish is covered by existing offences in other legislation.

75 Gilbert + Tobin Centre of Public Law, *Submission 2*; Dr Greg Carne, *Submission 5*; Media, Entertainment & Arts Alliance, *Submission 6*; Law Council of Australia, *Submission 13*; Joint media organisations, *Submission 17*; Professor A J Brown, *Submission 19*; Ms Alison Bevege, *Submission 23*; Australian Human Rights Commission, *Submission 28*; Mr Geoff Taylor, *Submission 29*.

3.105 These issues were addressed in detail by the Department and ASIO in a supplementary submission to the inquiry.[76]

3.106 The IGIS raised two more specific concerns in her submission related to possible unintended consequences in the offence provisions contained in both Schedule 3 and Schedule 6 to the Bill. Firstly, the IGIS expressed concern that due to an absence of clear statutory authority in the Bill for individuals to 'provide information to the IGIS for the purpose of complaints and inspections', complainants may not be clear on whether the legislation allows them to disclose information to the IGIS or her staff:

> While the heads of each intelligence agency have indicated that it is not their intention to limit the disclosure of information to the IGIS or IGIS staff … it is not satisfactory for complainants, disclosers or IGIS staff to rely on such express or implied agreement. There should be clear statutory authority for individuals to provide information to the IGIS for the purpose of complaints and inspections under the IGIS Act, notwithstanding other laws, agreements or undertakings.[77]

3.107 The second issue raised by the IGIS was that staff of the office of the IGIS may 'inadvertently be subject to this secrecy provision in relation to information they acquire when inspecting agency records'. Coupled with the provisions in proposed section 35P relating to the SIO scheme, which 'appear absolute in their terms', the IGIS was concerned about the unintended impact the Bill may have on the internal functioning of her office:

> [T]here should be no doubt that information that IGIS staff identify during their inspection activity can be conveyed to the IGIS and to other IGIS staff in the course of their duties.[78]

3.108 At a public hearing, the IGIS reiterated her firm preference for any doubt about these matters to be explicitly clarified in the legislation.[79]

3.109 In his submission, Dr Greg Carne of the University of New England similarly called for a specific exemption to be included in the proposed

---

76 Attorney-General's Department and ASIO, *Submission 1.2*, pp. 74–83.

77 IGIS, *Submission 4*, p. 20.

78 IGIS, *Submission 4*, p. 20. The submission explained that IGIS staff are sometimes required to sign an agreement with an agency before accessing their information, which could mean that they meet the broad definition of 'entrusted person' in proposed section 18A(5).

79 Dr Thom, IGIS, *Committee Hansard*, Canberra, 15 August 2014, p. 6.

offence provisions for activities done 'as part of, or in preparation for, disclosure to the [IGIS] under sections 26, 33 and 34 of the [PID Act]'.[80]

3.110 The Attorney-General's Department and ASIO responded to the concerns raised by participants in a supplementary submission to the inquiry. The submission addressed the necessity of the Schedule 6 offence provisions, the lack of a 'harm' requirement, the size of the proposed penalties, and other matters. The Department argued against any changes to the Bill in regard to these matters.[81]

3.111 In relation to the work of the IGIS, the Department and ASIO maintained that disclosures to the IGIS by 'entrusted persons' would not be captured by the proposed offences in Schedule 6, as such disclosures would be considered to be 'authorised'. The organisations noted that the PID Act and IGIS Act each provide immunity from liability to secrecy offences for complaints or disclosures to the IGIS. However, the Department and ASIO also acknowledged the IGIS's preference for this immunity to be explicit in the legislation, and agreed that 'it is important that the offences do not act as a barrier to disclosing information to, or cooperating with, the IGIS in the performance of her statutory function'. The Department and ASIO indicated they would examine possible amendments to give effect to the IGIS's preference.[82]

Committee comment

3.112 The Committee appreciates the necessity of offences for unauthorised handling and communication of information held by intelligence agencies, and recognises the Bill's intent to close legislative gaps and strengthen the integrity of the existing secrecy provisions.

3.113 However, the Committee is concerned that the offence provisions of the Bill, as drafted, could have unintended consequences relating to the legitimate disclosure of information to (and within) the IGIS. Given the inherently restricted environment within which intelligence agencies operate, clearly authorised avenues for employees and affiliates of those agencies to make complaints to the IGIS are essential. It is important that not only does the law allow for complaints to be made to the IGIS, but for this to be explicit in the legislation so that individuals have no doubt as to whether or not they are breaking the law when making a complaint. The very fact that there are differing views about the Bill's preservation of

80 Dr Greg Carne, *Submission 5*, p. 14.

81 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 74–83.

82 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 48–49.

existing public interest disclosure protections indicates that more explicit assurances are needed.

3.114 The Committee supports the IGIS's proposal to make explicit in the Bill that the proposed offence provisions in Schedule 6 do not apply to the disclosure of information by 'entrusted persons' to the IGIS or her staff. The Committee also calls for the possible unintended consequence of some staff of the Office of the IGIS not being able to disclose information to the IGIS or her other staff to be rectified in the final Bill. The Committee notes the proposals made by the Department to address the IGIS's concerns.

Recommendation 14

The Committee recommends that the National Security Legislation Amendment Bill (No. 1) 2014 be amended to confirm that the offence provisions in Schedule 6 to the Bill do not apply to

- **information disclosed to the Inspector-General of Intelligence and Security (IGIS) in the course of inspections, or in support of a complaint or other pro-active disclosure, or**
- **communication of information by IGIS staff to the IGIS or other staff within the Office of the IGIS in the course of their duties.**

ASIS cooperation with ASIO

3.115 As outlined in Chapter 2, the Bill proposes to add a new function to the Australian Secret Intelligence Service (ASIS)'s powers under the *Intelligence Services Act 2001* (the IS Act) that would allow it to collect intelligence on Australians overseas without first receiving ministerial authorisation, when done at the request of ASIO (when practicable) and in support of ASIO's functions.

3.116 In a public submission to the inquiry, ASIS declared that it was 'in Australia's national interest' for Australia's foreign intelligence and security services to be able to 'interact and work seamlessly together'. It explained that the purpose of the new provisions was to 'better enable ASIS to assist ASIO overseas', and that the effectiveness of this had been limited in the past due to the differences in the legislative frameworks of the two organisations:

> Experience with the different legislative regimes applying to ASIS and ASIO has identified situations where ASIO could properly collect intelligence on an Australian person because it would be relevant to security, but ASIS cannot assist ASIO in collecting that intelligence. There are also situations where, even though ASIS can obtain an emergency ministerial authorisation under the current provisions of the [IS Act], the realities of operating in high threat areas mean that the opportunity to act quickly on the basis of that authorisation may have been lost.[83]

3.117 ASIS indicated that the amendment would only apply to less intrusive activities overseas, for which ASIO would not be required to obtain a warrant if they were conducted in Australia.[84]

3.118 Some participants in the inquiry raised concerns that the proposed amendment, by removing the requirement for ministerial authorisation, would reduce accountability and weaken the existing limitations on ASIS's remit. Particular concern was raised about the proposed ability for ASIS, in limited circumstances, to collect intelligence on an Australian in support of ASIO without having first received a request from ASIO.[85]

3.119 In their appearance before the Committee, the Councils for Civil Liberties across Australia queried whether or not more effective collaboration between ASIO and ASIS could be achieved by other means.[86] In a supplementary submission, the Councils argued that the proposed shift towards internal authorisation was 'a major weakening of the existing safeguard' because of the breadth of the criteria that would need to be met to permit ASIS activity in support of ASIO.[87]

3.120 Other submitters noted that the proposed amendment would go some way to rectifying an existing anomaly where the level of protection over the privacy rights of Australians may depend on the particular intelligence agency involved.[88] While supportive of the more consistent approach and the safeguards proposed in the Bill, the Law Council of Australia suggested that those safeguards would be strengthened by specifying

---

83 ASIS, *Submission 8*, p. 2.

84 ASIS, *Submission 8*, p. 2.

85 Gilbert + Tobin Centre of Public Law, *Submission 2*; Associate Professor Greg Carne, *Submission 5*; Electronic Frontiers Australia, *Submission 9*; Australian Human Rights Commission, *Submission 28*.

86 Dr Lynch, NSW Council for Civil Liberties, *Committee Hansard*, Canberra, 18 August 2014, p. 21.

87 Councils for Civil Liberties across Australia, *Supplementary Submission 20.1*, p. 3.

88 IGIS, *Submission 4*; Law Council of Australia, *Submission 13.*

'what types of "activities" could be approved, how long the approval would be for, and on what basis it could be approved or renewed'.[89]

3.121 At a public hearing, the IGIS reiterated her suggestion to the previous Committee that 'whatever standard it is that the government considered appropriate should apply broadly to all of the agencies'. The IGIS noted that the proposed amendments would only result in a common standard for less invasive intelligence gathering activities. For other activities, such as the use of surveillance devices, the current regime would remain in place—that is, ASIS would require ministerial authorisation to perform activities overseas that would require a warrant in Australia, while ASIO would not.[90]

Committee comment

3.122 The Committee notes the removal of the requirement for ministerial authorisation for ASIS to collect intelligence on ASIO's behalf was not specifically recommended in its previous report. However, the measures proposed in the Bill are generally in line with the previous Committee's recommendation for a common standard (based on the ASIO Act) to apply to the authorisation of intrusive activities by ASIO and the IS Act agencies overseas. In fact, as the proposed alignment only applies to ASIO and ASIS and does not apply to activities that would otherwise require a warrant to be carried out in Australia, the proposal falls short of the 'common standard' that was envisaged.

3.123 The Committee considers that the proposed amendment should not be seen as an expansion of ASIS's functions beyond its remit, as some participants suggested, but rather as a means to better facilitate cooperation with ASIO in areas where the functions of the two organisations overlap. The increasing number of Australians who are travelling overseas to fight in foreign conflicts has been identified as a key long term challenge for Australia's counter-terrorism effort. In this environment, ASIO's ability to leverage the existing sources of overseas intelligence available to ASIS is increasingly important, and responds to a situation not necessarily envisaged when the IS Act was originally drafted.

3.124 The Committee recognises that the sensitive environments in which ASIS officers work means that there will, at times, be situations in which obtaining a written request from ASIO to collect intelligence on an Australian person of security interest (using non-invasive means) will not

89 Law Council of Australia, *Submission 13*, p. 50.

90 Mr Blight, Office of the IGIS, *Committee Hansard*, Canberra, 15 August 2014, p. 5.

be practicable. The Committee accepts that ASIS's ability to seize such opportunities, which may have serious security implications, should not be compromised by inflexible legislative requirements. The Committee therefore supports the proposed provision for ASIS to collect intelligence without a formal request from ASIO in these limited circumstances. It is appropriate that the use of this power should be subject to independent scrutiny, and as such the Committee supports the Bill's requirement for the IGIS to be notified as soon as practicable in each instance.

Oversight and scrutiny

IGIS resourcing

3.125 During the inquiry, some participants raised concerns about the Office of the IGIS's limited capacity to perform its new oversight responsibilities, including in relation to the new powers included in the Bill, with its current Budget allocation.[91] For example, Associate Professor Greg Carne argued that it would be timely for a 'comprehensive audit' of the supervisory and monitoring roles of the IGIS (and the Independent National Security Legislation Monitor), with a view to

> fixing in legislation a minimum budgetary allocation … representing a mathematical proportion of the overall budgetary appropriation to the members of Australia's intelligence community.[92]

3.126 The submission from the IGIS stated that the amendments proposed in the Bill would 'increase the scope and complexity of oversight arrangements and the workload of the [Office of the] IGIS'. The submission then listed the range of new powers in the Bill that would require additional oversight.[93]

3.127 At her appearance before the Committee, the IGIS noted that the Prime Minister had recently announced the Government would be increasing the resources for the Office of the IGIS. The IGIS explained that while the exact amount had not yet been determined, her estimate was that up to five additional people, at an annual cost of around $700 000, would be

91 Associate Professor Greg Carne, *Submission 5*; Ms Alison Bevege, *Submission 23*; Mr Keim, Law Council of Australia, *Committee Hansard*, Canberra, 18 August 2014, p. 3.

92 Associate Professor Greg Carne, *Submission 5*, p. 3.

93 IGIS, *Submission 4*, p. 3.

needed provide adequate oversight of the new powers proposed in the Bill. The additional resources would need to take into account the increased technical complexity of the Office's work, particularly as a result of the proposed changes to the computer access warrants regime.[94]

3.128 Apart from the need for additional resources and technical expertise, the IGIS agreed that there were no major issues that would prevent her from providing adequate oversight of the proposed new powers in the Bill:

> We are saying these new powers could be oversighted under the existing regime, under our existing legislation, but we would have to change the way that we do it.[95]

Committee comment

3.129 The Committee recognises the importance of having a strong regime in place to provide oversight over the activities of Australia's intelligence and security organisations. Those activities are, rightly, not subject to the same transparency requirements and opportunities for public scrutiny as other agencies, meaning the role of the IGIS is particularly important. However, at a time when intelligence and security organisations are growing significantly, both in their size and in the scope of their powers, the need for a concurrent boost in the capabilities of the IGIS is clear.

3.130 The Committee notes the IGIS's evidence that she has sufficient authority under existing legislation to oversight the new powers proposed in the Bill, but that there would be resource implications as a result of increased workload and complexity of oversight.[96]

3.131 The Committee welcomes the Prime Minister's recent announcement that the Government will increase the resources allocated to the IGIS to ensure proper oversight of the new powers and resources being allocated to intelligence agencies.[97] While acknowledging the current tight financial situation, the Committee considers that it is critical that budget supplementation for the Office of the IGIS takes into account the additional need for oversight associated with this Bill, including the Committee's recommended amendments to the SIO scheme and in regard to use of force provisions during the execution of ASIO warrants.

---

94 Dr Thom, IGIS, *Committee Hansard,* Canberra, 15 August 2014, pp. 1, 3.

95 Dr Thom, IGIS, *Committee Hansard,* Canberra, 15 August 2014, p. 7.

96 IGIS, *Submission 4*, p. 3; Dr Thom, IGIS, *Committee Hansard,* Canberra, 15 August 2014, p. 7.

97 The Hon Tony Abbott MP, Prime Minister and Senator the Hon George Brandis QC, Attorney-General, 'New counter-terrorism measures for a safer Australia', *Media Release*, 5 August 2014.

3.132 The Committee further considers that, while the IGIS has indicated she has the legislative authority needed to provide oversight over the current Bill, subsequent legislation announced by the Government may mean that it is necessary to strengthen the IGIS's capacity beyond that which has been committed already.

Recommendation 15

The Committee recommends that the Office of the Inspector-General of Intelligence and Security's annual budget be supplemented to the extent required to provide for the new oversight requirements associated with the National Security Legislation Amendment Bill (No. 1) 2014, including periodic reviews of special intelligence operations and oversight of the use of force during the execution of warrants.

Supplementation of the Office of the Inspector-General of Intelligence and Security's budget should also take other proposed measures to expand the powers of intelligence agencies into account.

Scrutiny of legislation

3.133 On 19 March 2014, legislation was introduced into the House of Representatives to abolish the position of the Independent National Security Legislation Monitor.[98] However, on 16 July 2014, the Attorney-General announced that the position would now be retained in light of the introduction of the National Security Legislation Amendment Bill (No. 1) 2014 into the Senate and 'potential further changes stemming from the Government's comprehensive review of Australia's national security legislation'.[99]

3.134 Some inquiry participants, while welcoming the Government's decision to continue funding the Independent National Security Legislation Monitor role, expressed concerns about the current vacancy in the position.[100]

3.135 Many participants also raised concerns about the short timeframe allocated for the Committee's inquiry.[101]

98 Independent National Security Legislation Monitor Repeal Bill 2014.

99 Senator the Hon George Brandis QC, Attorney-General, 'National Security Legislation Amendment Bill (No. 1) 2014', *Media release*, 16 July 2014.

100 Associate Professor Greg Carne, *Submission 5*; Australian Lawyers Alliance, *Submission 7*; Guardian Australia, *Submission 12*;Law Council of Australia, *Submission 13*; Mr Bruce Baer Arnold, *Submission 14*; Senator David Leyonhjelm, *Submission 15*; Dr Lesley Lynch, NSW Council for Civil Liberties, Canberra, *Committee Hansard*, 18 August 2014, p. 18.

Committee comment

3.136 The Committee welcomes the recent announcement that the position of Independent National Security Legislation Monitor will be retained.[102] Given the increase in terrorist threats and security concerns which have given rise to the measures proposed in the Bill, it is important to ensure a sound regime of ongoing legislative scrutiny. The establishment of an independent reviewer position was a key recommendation made in December 2006 by one of this Committee's predecessors. That recommendation followed a comprehensive review of security and counter-terrorism legislation that also took into account the findings of the independent Security Legislation Review Committee (the 'Sheller Committee').[103] The Committee considers that the changes to Australia's national security and anti-terror laws proposed in this Bill and those anticipated in future Bills warrant the current vacancy in this important position being filled as soon as practicable.

Recommendation 16

The Committee recommends that the Government appoint an Independent National Security Legislation Monitor as soon as practicable.

3.137 The Committee considers that the opportunity to examine the Bill through public inquiry has been an important element of addressing community concerns and strengthening the effectiveness of the safeguards in the Bill. However, it notes that many participants felt the inquiry timeframe requested by the Attorney-General did not allow time for a fully comprehensive analysis of its provisions.

Concluding comments

3.138 In the previous Parliament, the Committee spent a significant amount of time conducting a public inquiry into many of the Bill's proposals. While

101 Gilbert + Tobin Centre for Public Law, *Submission 2*; Australian Lawyers Alliance, *Submission 7*; Electronic Frontiers Australia, *Submission 9*; Law Council of Australia, *Submission 13*; Pirate Party of Australia, *Submission 18*; Councils of Civil Liberties across Australia, *Submission 20*; Muslim Legal Network (NSW) and Birchgrove Legal, *Submission 21*; Blueprint for Free Speech, *Submission 22*.

102 Senator the Hon George Brandis QC, Attorney-General, 'National Security Legislation Amendment Bill (No. 1) 2014', *Media Release*, 16 July 2014.

103 PJCIS, *Review of Security and Counter Terrorism Legislation*, December 2006.

the timeframe for the inquiry into this Bill has been constrained, the Committee has still received a considerable number of submissions and conducted both public and private hearings. The Committee also notes that this report is designed to inform the further debate that will take place when the Bill is considered by the Parliament.

3.139 The Committee notes that not all of its predecessor's recommendations were accepted fully by the Government. However, the Committee sought through this inquiry to judge the effectiveness of the provisions of the Bill on their own merits, rather than revisiting their policy intent.

3.140 The Committee appreciates the contribution of all involved in the inquiry and notes that all public evidence received is available on the Committee's website. This report provides a summary of the main issues raised. The issues raised by inquiry participants who made submissions and spoke with the Committee at hearings were instrumental in framing the Committee's subsequent discussions with the Department and its work to introduce additional safeguards and clarifications to address the areas of most concern.

3.141 The Committee also thanks the Attorney-General's Department and ASIO for their high level of engagement with the inquiry, and in particular for the thoroughness of their responses to concerns raised by stakeholders. The Committee encourages other participants in the inquiry to review the supplementary material that the Department and ASIO have provided, which directly responded to the many of the issues raised in submissions and at hearings.

3.142 The Committee also notes that there were a small number of additional issues addressed in the Department and ASIO's supplementary submission for which the organisations have suggested 'avoidance of doubt' style provisions that could be included in the Bill or further information in the Explanatory Memorandum that could be considered.[104] While these additional matters were not subject to close examination by the Committee in the inquiry, the Committee encourages the Government to act on the suggestions it has made in order to provide additional clarity where it is needed. The Committee also supports the Department and

104 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*. The suggestions included a provision or note in the Bill expressly stating the relationship between proposed sections 35K and 35L in the Bill relating to SIOs, or setting this out in the Explanatory Memorandum (p. 43); the addition of an express provision in section 35F in the Bill or in the Explanatory Memorandum to avoid any doubt that the issuing criteria for SIOs must continue to be satisfied when SIOs are varied (p. 45); and additional material in the Explanatory Memorandum regarding protections in place to ensure the privacy of information shared by ASIO with the private sector (pp. 69–70).

ASIO's more general undertaking to examine potential improvements to the Explanatory Memorandum to 'assist in the understanding of the legislative package'.[105]

3.143 The Committee supports the intent of the Bill to increase the effectiveness of Australia's intelligence organisations at a time when the threat to our country and its interests from terrorism remains high.

3.144 The Committee emphasises the importance of effective monitoring and scrutiny powers, and notes that the IGIS has confirmed she has sufficient authority to oversight the proposed new measures. The Committee also recognises that the proposed measures are broadly in line with the recommendations of its previous report.

3.145 The new recommendations the Committee makes in this report are intended to strengthen the integrity of the Bill—that is, to improve safeguards and strengthen public confidence that the powers it extends cannot be used in a way that goes beyond their legitimate policy intent. Following consideration of the recommendations made in this report, the Committee recommends that the Bill be passed by the Parliament:

Recommendation 17

The Committee recommends that, following consideration of the recommendations in this report, the National Security Legislation Amendment Bill (No. 1) 2014 be passed by the Parliament.

Mr Dan Tehan MP
Chair
September 2014

105 Attorney-General's Department and ASIO, *Supplementary Submission 1.2*, pp. 51–52.

A

Appendix A – List of Submissions and Exhibits

Submissions

1. Attorney-General's Department
   - 1.1. Supplementary
   - 1.2. Supplementary (joint submission with the Australian Security Intelligence Organisation)
   - 1.3. Supplementary
2. Gilbert + Tobin Centre of Public Law
   - 2.1. Supplementary
3. Mr Bill Calcutt
   - 3.1. Supplementary (CONFIDENTIAL)
4. Inspector-General of Intelligence and Security
   - 4.1. Supplementary
5. Dr Greg Carne
6. Media, Entertainment & Arts Alliance
7. Australian Lawyers Alliance
8. Australian Secret Intelligence Service
9. Electronic Frontiers Australia, Inc.
   - 9.1. Supplementary
10. Australian Crime Commission
11. Office of the Australian Information Commissioner
    - 11.1. Supplementary
12. Guardian Australia
13. Law Council of Australia

14. Mr Bruce Baer Arnold
15. Senator David Leyonhjelm
16. Australian Security Intelligence Organisation
17. Joint media organisations
18. Pirate Party Australia
19. Professor A J Brown
20. Civil Liberties Councils across Australia
    - 20.1. Supplementary
21. Muslim Legal Network (NSW) and Birchgrove Legal
    - 21.1. Supplementary
22. Blueprint for Free Speech
23. Ms Alison Bevege
    - 23.1. Supplementary (CONFIDENTIAL)
24. Dr Asmi Wood
25. Australian Privacy Foundation
26. Australian Interactive Media Industry Association – Digital Policy Group – Cyber-Safety and Security Sub-Group
27. Civil Liberties Australia
28. Australian Human Rights Commission
29. Mr Geoff Taylor
30. CONFIDENTIAL

Exhibits

1. Telstra Corporation

B

Appendix B – Witnesses appearing at private and public hearings

Friday, 15 August 2014 – Canberra, ACT (private hearing)

Australian Secret Intelligence Service

Mr Nick Warner, Director-General
Deputy Director-General, Operations
Deputy Director-General, Capability and Corporate Management
General Counsel

Friday, 15 August 2014 – Canberra, ACT (public hearing)

Attorney-General's Department

Ms Jamie Lowe, A/g First Assistant Secretary, National Security Law and Policy Division
Ms Annette Willing, National Security Legal Advisor, National Security Law and Policy Division
Ms Christina Raymond, Senior Legal Officer, National Security Law and Policy Division

Australian Security Intelligence Organisation

Mr David Irvine AO, Director-General
Ms Kerri Hartland, Deputy Director-General

Office of the Inspector-General of Intelligence and Security

Dr Vivienne Thom, Inspector-General of Intelligence and Security
Mr Jake Blight, Assistant Inspector-General of Intelligence and Security

Monday, 18 August 2014 - Canberra, ACT (public hearing)

Australian Lawyers Alliance

Mr Greg Barns, spokesperson and former National President

Civil Liberties Councils across Australia

Dr Lesley Lynch, Secretary, NSW Council for Civil Liberties
Mr Bill Rowlings OAM, CEO, Civil Liberties Australia

Electronic Frontiers Australia

Mr Jon Lawrence, Executive Officer
Dr Roger Clarke, Life Member

Gilbert + Tobin Centre of Public Law

Professor George Williams
Dr Nicola McGarrity
Mr Keiran Hardy

Law Council of Australia

Mr Stephen Keim SC, Member of the Law Council's National Human Rights Committee
Ms Leonie Campbell, Co-Director, Criminal Law and Human Rights Division
Dr Natasha Molt, Policy Lawyer, Criminal Law and Human Rights Division

Media, Entertainment & Arts Alliance

Mr Christopher Warren, Federal Secretary
Mr Mike Dobbie, Communications Manager, Media Section

Office of the Australian Information Commissioner

Mr Timothy Pilgrim, Privacy Commissioner
Ms Angelene Falk, Assistant Commissioner

Monday, 18 August 2014 – Canberra, ACT (private hearing)

Attorney-General's Department

Mr Michael Rothery, A/g Deputy Secretary, National Security and Criminal Justice Group

Ms Annette Willing, National Security Legal Advisor, National Security Law and Policy Division
Ms Christina Raymond, Senior Legal Officer, National Security Law and Policy Division

Australian Security Intelligence Organisation

Ms Kerri Hartland, Deputy Director-General
Deputy Director-General
First Assistant Director-General, Corporate and Security
First Assistant Director-General, Counter Espionage and Interference
First Assistant Director-General, Office of Legal Counsel
Assistant Director-General, Legislation, Warrants and Technical Capabilities