2

IS BILL – PART 2—Functions of the agencies

Background

2.1 Part 2 of the IS Bill is significant in that it sets out in legislation, for the first time, the functions of both ASIS and DSD under clauses 6 and 7. Clauses 8 and 9 provide the framework for Ministerial directions and authorisations. In addition, the Inspector-General of Intelligence and Security (IGIS) has oversight powers in relation to Ministerial directions and authorisations.

2.2 Clauses 11 and 12 place limits on agencies' functions and activities. Clause 14 provides liability for certain acts.

2.3 Clause 15 sets out rules to protect privacy of Australians. The objective of this clause is to require that agencies take all possible measures to ensure that their activities are undertaken with due regard to the rights of Australians to privacy.

2.4 These aspects of the IS Bill are examined in this chapter. The relevant clauses are described and, where necessary, information in the explanatory memorandum is used to further clarify the intentions of the clauses. The analysis section includes a discussion of evidence received in submissions and through public hearings. We conclude with our own comments and recommendations where necessary.

Clause 6 – Functions of ASIS

2.5 Clause 6 is divided into three subclauses. The Explanatory Memorandum (EM) states that subclauses (1)(a) to (d) 'reflect the central functions of ASIS. Clause 6 is produced, in full, below:

6 Functions of ASIS

(1) The functions of ASIS are:

(a) to obtain, in accordance with the Government's requirements, intelligence about the capabilities, intentions or activities of people or organisations outside Australia; and

(b) to communicate, in accordance with the Government's requirements, such intelligence; and

(c) to conduct counter-intelligence activities; and

(d) to liaise with intelligence or security services, or other authorities, of other countries; and

(e) to undertake such other activities as the responsible Minister directs relating to the capabilities, intentions or activities of people or organisations outside Australia.

(2) The responsible Minister may direct ASIS to undertake activities referred to in paragraph (1)(e) only if the Minister:

(a) has consulted other Ministers who have related responsibilities; and

(b) is satisfied that there are satisfactory arrangements in place to ensure that, in carrying out the direction, nothing will be done beyond what is necessary having regard to the purposes for which the direction is given; and

(c) is satisfied that there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in carrying out the direction will be reasonable having regard to the purposes for which the direction is given.

(3) A direction under paragraph (1)(e) must be in writing.

(4) In performing its functions, ASIS must not plan for, or undertake, paramilitary activities or activities involving violence against the person or the use of weapons.

Note 1: For other limits on the agency's functions and activities see sections 11 and 12.

Note 2: If the Minister gives a direction under paragraph (1)(e), the Minister must give a copy of the direction to the Inspector-General of Intelligence and Security as soon as practicable after the

direction is given to the head of ASIS (see section 32B of the Inspector-General of Intelligence and Security Act 1986).

2.6 The EM indicates that paragraph 6(1)(e) 'provides a degree of flexibility for the Government in its tasking of ASIS' by allowing ASIS 'to undertake such other activities as the responsible Minister directs'. This power is subject to limited conditions which are set out in subclause 6(2). In addition, subclause 6(3) states that any direction to perform 'other activities' as set out under 6(1)(e) 'must be in writing.'

2.7 Subclause 6(4) emphasises that ASIS must not be involved in para-military operations or activities involving personal violence or the use of weapons.

Analysis

2.8 The evidence suggested that clause 6 was positive in setting out in legislation the functions of ASIS. In particular, it was noted that subclause 6(4) served an important purpose in stating that ASIS cannot undertake paramilitary activities or conduct activities involving violence or the use of weapons. However, paramilitary activities was not defined in the Bill.

2.9 Concerns were raised about paragraph 6(1)(e) which provides the Minister with the power to direct ASIS to undertake 'such other activities' relating to the capabilities, intentions or activities of people or organisations outside Australia.' Mr Mark Weeding commented that the wording of 6(1)(e) does not provide a 'strong sense of accountability.'[1]

2.10 The accountability provisions applying to 6(1)(e) include the need for the responsible Minister to consult with other Ministers, and make the direction in writing which would be made available to the IGIS. During hearings, it was proposed that another form of accountability could apply by ensuring that a copy of a direction under 6(1)(e) be provided to the proposed Parliamentary Joint Committee on ASIO and ASIS. ASIS responded that it would not be opposed to this but it remains a policy decision for government.[2]

2.11 ASIS confirmed during hearings that clause 6 represents the functions of ASIS as set out in the current directive with the exception of 6(1)(e). ASIS indicated that ASIS has the authority to work against people traffickers which was agreed by the government and added to the directive. ASIS stated:

---

1 Mr Mark Weeding, *Transcript*, p. 2.

2 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 105.

> I think the way in which the functions are there defined reflects the current situation: 6(1)(e) reflects the fact that now government has the power to direct ASIS to carry out activities and that power to change the functions of ASIS by adding to them in that specific and limited way is protected in 6(1)(e) to meet any contingency that might arise in future. It is an attempt not to tie the hand of government in any contingency which might arise.[3]

2.12 The IGIS reported, in his submission, that the functions of ASIS as set out in the IS Bill and the functions in the current government directive are as reported by ASIS in evidence.[4]

Conclusions

2.13 It is noted that there were some concerns about paragraph 6(1)(e). While we accept that there is validity in the argument that there is the need for flexibility in the tasking of ASIS, stronger levels of accountability for 6(1)(e) are required. Currently, the provisions under 6(2) and 6(3) provide some controls on the application of 6(1)(e). All directions issued under 6(1)(e) will be in writing and provided to the IGIS. The IGIS would be obligated to address any concerns regarding directions given under 6(1)(e) if he believed that they were inconsistent with the broader provisions of the Intelligence Services Bill.

2.14 During hearings, it was proposed that real Parliamentary accountability could be achieved if a written direction under 6(1)(e) was provided to the proposed Parliamentary Joint Committee on ASIO and ASIS. The power of the Minister to direct ASIS to undertake 'other activities' is potentially wide and there is minimal accountability back to the Parliament. The Parliament's oversight of directions made under 6(1)(e) will provide sufficient safeguards against misuse of this provision.

3 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 73.

4 Inspector-General of Intelligence and Security, *Submission No. 13*, p. 1.

Recommendation 1

2.15 **Note 2 to Clause 6 of the Intelligence Services Bill 2001 be amended to read:**

- **If the Minister gives a direction under paragraph (1)(e), the Minister must as soon as practicable after the direction is given to the head of ASIS provide a copy of the direction to the Inspector-General of Intelligence and Security, *and advise the Parliamentary Joint Committee on ASIO and ASIS of the nature of the other activity to be carried out*.**

2.16 In those cases where the responsible Minister may activate 'other activities' under 6(1)(e) which relate to Australian citizens or Australian organisations overseas, then further accountability is required. This can be achieved through connecting the operation of 6(1)(e) to clauses 8 and 9 of the IS Bill which provide for Ministerial directions and authorisations.

Recommendation 2

2.17 **Clauses 8 and 9 of the Intelligence Services Bill 2001 be amended to require authorisation by the responsible Minister for "other activities" under clause 6(1)(e) relating to Australian persons or Australian organisations overseas; and**

- **that in giving any such authorisation under Section 9 the Minister must be satisfied that the Australian person or organisation overseas is engaged in, or is reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to Australia's national security;**
- **that the activity proposed to be authorised will directly enhance or protect Australia's national security;**
- **that any such authorisation have effect for six months, whereupon it will lapse unless renewed by the Minister.**

2.18 In relation to subclause 6(4), we recommend that the definition for 'paramilitary activities' should be included in clause 3-definitions. The

final chapter will include a recommendation dealing with this and the need for other definitions in the Bill.

Clause 7 – Functions of DSD

2.19 Clause 7 sets out the functions of DSD. Clause 7 is produced, in full, below:

7 Functions of DSD

The functions of DSD are:

(a) to obtain intelligence about the capabilities, intentions or activities of people or organisations outside Australia in the form of electromagnetic energy, whether guided or unguided or both, or in the form of electrical, magnetic or acoustic energy, for the purposes of meeting the requirements of the Government, and in particular the requirements of the Defence Force, for such intelligence; and

(b) to communicate, in accordance with the Government's requirements, such intelligence; and

(c) to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; and

(d) to provide assistance to Commonwealth and State authorities in relation to cryptography and communications technologies.

Note: For limits on the agency's functions and activities see sections 11 and 12.

Analysis

2.20 DSD confirmed that the functions in clause 7 reflect what is in the current directive.[5] The IGIS reported, in his submission, that the functions of DSD as set out in the IS Bill and the functions in the current government directive are as reported by DSD in evidence.[6]

2.21 The Australian Council for Civil Liberties (ACCL) expressed concerns with subclause 7(d) relating to the provision of cryptographic advice to Commonwealth and State authorities. The ACCL's view is that Australian

5 Mr Ron Bonighton, Defence Signals Directorate , *Transcript,* p. 54.

6 Inspector-General of Intelligence and Security, *Submission No. 13*, p. 1.

citizens should be entitled to use cryptography to protect the transmission of their private information. The ACCL claimed that the underlying objective of subclause 7(d) is about ensuring that citizens do not have encryption material that law enforcement agencies cannot decipher.[7]

2.22 DSD disagreed with this assessment, submitting that 7(d) provides for DSD to assist Commonwealth and State authorities to encrypt official communications to a sufficient standard.

2.23 DSD indicated that it had not provided cryptographic advice to a state police force 'but we could provide advice if they came to the AFP' and requested advice.[8] DSD stated:

> I think we can foresee a time when we might, as the decrypter of last resort, if you like, provide some assistance to state police forces, if there were serious offences. The fact is that a country like Australia would not be able to afford to set up the sort of capability that DSD possesses. Without going into any specific details, that is a simple fact. On the other hand, I am not at all interested in having a whole lot of decryption agencies going about without the sort of national security regime and discipline that we have built up over 50 years. I do not want to see unique techniques get out into the public domain.[9]

Conclusions

2.24 The Committee does not agree with the views about cryptography raised by the Australian Council for Civil Liberties, and, therefore, we do not support amending subclause 7(d). From an assurance perspective, however, there is cause for 7(d) to be scrutinised. The IGIS is well placed to conduct this role and report on the appropriateness of the advice provided in his annual report.

Recommendation 3

2.25 **The Inspector-General of Intelligence and Security should report, in his Annual Report, on the operation of subclause 7(d) of the Intelligence Services Bill 2001, once enacted.**

---

7 Mr Terry O'Gorman, Australian Council for Civil Liberties, *Transcript*, p. 37.

8 Mr Ron Bonighton, Defence Signals Directorate , *Transcript*, p. 50.

9 Mr Ron Bonighton, Defence Signals Directorate , *Transcript*, p. 54.

Clauses 8 and 9 – Ministerial directions and Ministerial authorisation

2.26 The EM indicates that 'certain activities conducted in pursuance of a function of an agency need to be approved by the Government. The directions issued under clause 8(1) specify those circumstances where an agency head must seek Ministerial authorisation in order to perform certain activities. The directions under this section are classified, although the IGIS will have oversight of agencies' compliance with Ministerial directions and authorisations.

2.27 Clause 9 provides the framework for the provision of Ministerial authorisations. A Minister in issuing an authorisation must be satisfied that the activities that will be performed are necessary for the proper performance of a function of the agency concerned. An Authorisation must be in writing and must specify the period for which the authorisation will have effect.

2.28 Clause 8 is produced, in full, below:

8 Ministerial directions

(1) The responsible Minister in relation to ASIS, and the responsible Minister in relation to DSD, must issue a written direction under this subsection to the relevant agency head. The direction must specify the circumstances in which the agency must, before undertaking particular activities or classes of activities, obtain an authorisation under section 9 from the Minister.

(2) The responsible Minister may give written directions to be observed:

(a) in the performance by the relevant agency of its functions; or

(b) in the case of ASIS—in the exercise of the powers of the Director-General under section 33 or 34.

(3) Each agency head must ensure that the agency complies with any direction given by the responsible Minister under this section.

(4) Directions under paragraph (2)(b) must not relate to a specific staff member.

Note: The Inspector-General of Intelligence and Security has oversight powers in relation to Ministerial directions and authorisations given under this Act. See in particular section 32B of the Inspector-General of Intelligence and Security Act 1986 (which requires the Minister to give a copy of a direction under this section to the Inspector-General of Intelligence and Security as soon as practicable after the direction is given).

2.29 Clause 9 is produced, in full, below:

9 Ministerial authorisation

(1) Before a Minister gives an authorisation under this section, the Minister must be satisfied that:

(a) any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned; and

(b) there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency; and

(c) there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

(2) The Minister may give an authorisation in relation to:

(a) an activity, or class of activities, specified in the authorisation; or

(b) acts of a staff member or agent, or a class of staff members or agents, specified (whether by name or otherwise) in the authorisation; or

(c) activities done for a particular purpose connected with the agency's functions.

(3) An authorisation is subject to any conditions specified in it.

(4) An authorisation must be in writing and must specify how long it will have effect.

(5) If a Minister gives an authorisation under this section in relation to an agency, the relevant agency head must ensure that a copy of the authorisation is kept by the agency and is available for inspection on request by the Inspector-General of Intelligence and Security.

Analysis

2.30 Clauses 8 and 9 provide a control framework by ensuring that certain activities of an agency are approved by Government. The IGIS will be provided with copies of all directions and authorisations. Clauses 8 and 9 are discussed in more detail below.

Clause 11 – Limits on agencies' functions

2.31 Clause 11 sets out limits on what the agencies can do. In particular, this clause states that the agencies' functions do not include policing or law enforcement. The EM confirms that while the agencies do not have a policing function, 'the agencies are permitted to obtain and communicate intelligence relevant to serious crime to police and law enforcement agencies.' Clause 11 is produced, in full, below:

11 Limits on agencies' functions

(1) The functions of the agencies are to be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.

(2) The agencies' functions do not include:

(a) the carrying out of police functions; or

(b) any other responsibility for the enforcement of the law.

However, this does not prevent the agencies from:

(c) obtaining intelligence under paragraph 6(1)(a) or 7(a) and communicating any such intelligence that is relevant to serious crime to the appropriate law enforcement authorities; or

(d) in the case of DSD—performing the function set out in paragraph 7(d).

(3) Subsection (1) does not apply to the functions described in paragraphs 7(c) and (d).

Analysis

2.32 The ACCL was critical of paragraph 11(2)(c). The ACCL suggests that the power of ASIS or DSD to acquire intelligence under paragraph 6(1)(a) and 7(a) and then to communicate knowledge of serious crime to the appropriate law enforcement agencies is an expansion of ASIS and DSD activities into ordinary criminal law. The IS Bill does not contain a definition of what constitutes 'serious crime'. This matter is addressed in chapter four.

2.33 The ACCL commented that paragraph 11(2)(c) 'represents a very considerable development in relation to the gathering of criminal

intelligence overseas for the use in Australia by domestic law enforcement agencies.'[10] The ACCL states:

> It is noted that nowhere in the second reading speech in relation to the Intelligence Services Bill 2001 is there a reference to the fact that both ASIS and DSD will be permitted to gather intelligence, not just on national security matters overseas but on matters pertaining to the ordinary criminal law.
>
> The uninitiated observer might counter that criminal intelligence gathering overseas is in relation to serious crime but as this concept is not defined, that is likely to be interpreted as most indictable offences.[11]

2.34 The ACCL concluded that the IS Bill will give 'very considerable powers to ASIS and DSD to gather criminal intelligence' and there is no prohibition in the Bill 'against questioning any of the activities of ASIS or DSD in Australian courts.'[12]

2.35 The ACCL was particularly concerned that criminal intelligence provided by either DSD or ASIS could be used to mount a criminal prosecution.[13] In addition, the ACCL suggested than any information or leads provided to a law enforcement agency may be withheld from the defence. The ACCL states:

> If the information gathered by ASIS was, say, from their own telephone tap and if the information of that telephone tap were known to the defence and could be put in front of a jury, it may well put a different interpretation on the later telephone tap that the NCA or the AFP mount against that target. In other words, ASIS might have gathered criminal intelligence which, if it were known to the defence that it existed, the defence could use to say, 'This is not what the prosecution evidence would have you, the jury, believe is the case.'[14]

2.36 In view of this, the ACCL suggested that the IGIS should be subject to requests by defence counsel, by way of subpoena, to 'look at ASIS and its intelligence gathering in a particular case to see whether there is something relevant that might be exculpatory to the defence'.[15] The

10 Australian Council for Civil Liberties, *Submission No 10*, p. 3.
11 Australian Council for Civil Liberties, *Submission No 10*, p. 3.
12 Australian Council for Civil Liberties, *Submission No 10*, p. 6.
13 Mr Terry O'Gorman, Australian Council for Civil Liberties, *Transcript*, p. 26.
14 Mr Terry O'Gorman, Australian Council for Civil Liberties, *Transcript*, p. 28.
15 Mr Terry O'Gorman, Australian Council for Civil Liberties, *Transcript*, p. 29.

concern was raised that this could lead to hundreds of requests to IGIS, most of which would have no substance.

2.37 The IGIS commented that in the hypothetical situation that an agency did withhold information significant to a defence, then he would take action. The IGIS stated:

> But let us suppose that we reach the hypothetical situation advanced by Mr O'Gorman—namely, that there is material revealed in intelligence collected by one of the agencies that could be suggestive that the individual concerned is not guilty of the crime of which they have been accused. My view would be that, if there were such material, it would be the duty of the organisation concerned to pass it on to the people responsible for law enforcement, and I would regard it as an issue of propriety within the terms of my legislation to ensure that that happened, provided that the information was significant.[16]

2.38 The ACCL, in a supplementary submission, proposed that in all cases where criminal intelligence is communicated to law enforcement agencies under 11(2)(c), then a copy of the communication should be provided to the IGIS.[17] In addition, the ACCL indicated that this should also apply to ASIO therefore suggesting an amendment to the ASIO Act.

2.39 The IGIS currently monitors ASIS and DSD to ensure that they comply with the 'nationality rules'. The nationality rules comprise *Rules for the Retention and Communication by ASIS of Foreign Intelligence Information Concerning Australian Persons*, and in relation to DSD *Rules on Foreign Signals Intelligence and Australian Persons.*[18] The IGIS reported that ASIS must not collect, retain or disseminate information about Australians except in certain limited circumstances. One example of such a circumstance is the communication of information about serious crime. The nationality rules 'require that ASIS record instances of collection and reporting on Australians, and provide the records to the IGIS for inspection. The IGIS reported:

> I undertook regular inspections, both of those records and of the reports themselves. In addition, my office conducted a cross-check of ASIS reporting, to which we have on-line access, to see whether

16 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 42.

17 Australian Council for Civil Liberties, *Submission No. 14*, p. 1.

18 Inspector-General of Intelligence and Security, *Annual Report, 1998-99,* pp. 20-23.

> ASIS is effectively identifying all instances of reporting on Australians.[19]

2.40 A similar framework for monitoring DSD's compliance with the nationality rules operates.[20] It is through these processes that the IGIS could ensure that any information relevant to a prosecution would be made available to the relevant legal authorities.

2.41 The point was made during hearings that if ASIS or DSD passed on criminal information to appropriate law enforcement authorities then those authorities could only use that information as a lead. These authorities would need to develop their own evidentiary case. The IGIS stated:

> If ASIS, or DSD for that matter, became aware of information that they then passed on to Australian law enforcement authorities and down the track there was a prosecution, first of all, as more than one of you have said, there needs to be admissible evidence for the prosecution to be launched, and that needs obviously to arise from things other than provided by the intelligence and security agencies.[21]

2.42 In opposition to the view that ASIS or DSD might be involved in gathering criminal intelligence, the Bill is clear on the functions of the agencies and their limitations. Paragraph 6(1)(a) states that the functions of ASIS are 'to obtain, in accordance with the Government's requirements, intelligence about the capabilities, intentions or activities of people or organisations outside Australia'. The ACCL argued that 'intelligence' in 6(1)(a) was not defined to mean national security intelligence.[22]

2.43 However, subclause 11(1) states that 'the functions of the agencies are to be performed only in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia.' On this point, the ACCL argues that 'national security' and 'economic well-being' are not defined. In addition, the ACCL suggested that 'police functions' should be defined. [23] It is noted that the ASIO Act contains a definition of 'security'.

---

19 Inspector-General of Intelligence and Security, *Annual Report, 1998-99,* p. 21.

20 Inspector-General of Intelligence and Security, *Annual Report, 1998-99,* p. 21.

21 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 42.

22 Mr Terry O'Gorman, Australian Council for Civil Liberties, *Transcript*, p. 28.

23 Mr Terry O'Gorman, Australian Council for Civil Liberties, *Transcript*, p. 35.

2.44 In addition, the ACCL suggested that because the Government's Directive is secret it is not possible to remove the possibility that criminal matters are included.

2.45 DSD and ASIS, during evidence, confirmed that the functions in the IS Bill were an accurate representation of what exists in the Directive. The IGIS, in a supplementary submission, compared the evidence given by the agencies and what exists in the Directive. The IGIS confirmed the advice given by DSD and ASIS.[24]

2.46 In response to the ACCL's suggestion that ASIS through ASIO could tap an Australian's phone and seek to obtain criminal intelligence, it was suggested that this would be inconsistent with the functions of the agencies. In addition, any warrants for phone tapping or Ministerial directive under paragraph 6(1)(e) would be subject to scrutiny by the IGIS.

2.47 The IGIS confirmed that ASIS does not have the legislative power to tap phones in Australia. The IGIS stated that 'the responsibility for telephone interception lies with ASIO pursuant to warrants approved by the Attorney-General.'[25]

Conclusions

2.48 It is proper and correct that ASIS or DSD should, in performing their functions and where criminal intelligence is inadvertently gathered, communicate intelligence of serious crime to the appropriate law enforcement authorities. The functions of ASIS and DSD, as set out in the functions and limitations of the IS Bill, are not to gather criminal intelligence. Any knowledge gathered by these organisations is by-product of their intelligence collection on national security issues.

2.49 The Australian Council for Civil Liberties (ACCL) has brought attention to the process for communicating intelligence on serious crime to law enforcement agencies. The ACCL's major concern is that where a prosecution arises from leads provided by ASIS or DSD, the defence against the prosecution may be excluded from vital information. The ACCL commented that law enforcement agencies cannot be relied upon to fulfil their duty of disclosure.

2.50 The ACCL proposed that this problem could be alleviated by ensuring that a copy be sent to the IGIS of any communication of criminal intelligence under paragraph 11(2)(c). Through this process the IGIS

24 Mr Bill Blick, Inspector-General of Intelligence and Security, *Submission No. 13*, p. 1.

25 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 42.

would automatically be made aware of these communications, and, if necessary, he could take appropriate action. In our view, such a process would duplicate the processes that already exist in relation to IGIS monitoring of the nationality rules for both ASIS and DSD. Under the nationality rules, both DSD and ASIS are required to record instances of collection and reporting on Australians, and provide the records to the IGIS. This includes instances where the agencies communicate criminal intelligence to the appropriate law enforcement agencies.

2.51 The Committee understands that the nationality rules will be enhanced through the operation of clause 15. This process should address the concerns raised by the ACCL.

Recommendation 4

2.52 **Clause 15 of the Intelligence Services Bill 2001 be amended to require the responsible Minister in relation to ASIS, and the responsible Minister in relation to DSD, to consult with the Attorney-General before making the rules relating to the communication and retention of information concerning Australian persons.**

Clause 14 – Liability for certain acts

2.53 Clause 14 provides for immunity from civil and criminal liability for ASIS or DSD. The EM states:

> The purpose of the clause is to provide immunity in a limited range of circumstances directly related to the proper performance by the agencies of their function. It does not provide a blanket immunity from Australian laws for all acts of the agencies. This limited immunity is necessary as certain Australian law, including State and Territory law, could impose liability on the agencies.

2.54 Clause 14 is produced, in full, below:

14 Liability for certain acts

(1) A staff member or agent of an agency is not subject to any civil or criminal liability for any act done outside Australia if the act is done in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for any act done inside Australia if:

(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and

(b) the act:

(i) involves aiding, abetting, counselling, procuring or otherwise planning or attempting to carry out; or

(ii) is otherwise directly connected with;

some other act outside Australia that would amount to an offence if that other act were committed in Australia; and

(c) the act is done in the proper performance of a function of the agency.

(3) In this section:

***act** includes omission.*

***staff member** includes the Director and the Director-General.*

2.55 The examination of clause 14 is undertaken together with an examination of the proposed amendments to the Criminal Code Act relating to ASIS and DSD contained in the Cybercrime Bill (hereafter referred to as division 476.5)

2.56 The relevant clauses of division 476.5 are almost identical to clause 14 in the IS Bill but make reference to 'computer related acts'. Subclauses 1 and 2 of division 476.5 are produced, in full, below:

476.5 Liability for certain acts

(1) A staff member or agent of ASIS or DSD(the agency) is not subject to any civil or criminal liability for any computer-related act done outside Australia if the act is done in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for any act done inside Australia if:

(a) the act (the ancillary act) is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and

(b) the ancillary act:

(i) involves aiding, abetting, counselling, procuring or otherwise planning or attempting to carry out; or

(ii) is otherwise directly connected with;

a computer-related act outside Australia that would amount to an offence against a law of the Commonwealth, a State or a Territory if that computer-related act were committed in Australia; and

(c) the ancillary act is done in the proper performance of a function of the agency.

2.57 The issue of immunity for staff of ASIS and DSD was the most controversial aspect of the Bills under examination. ASIS and DSD justified the need for clause 14 on the grounds of 'global technological change and laws that have been passed in Australia that can have application overseas.'[26] ASIS stated:

> In cases where there was concern that a proposed ASIS activity could raise difficulties under Australian law, ASIS has sought legal advice. Where this advice has indicated that ASIS could be in breach of Australian law if the activity proceeded, ASIS has not undertaken the activity. This has resulted in the loss of intelligence required by Government.[27]

2.58 Similarly, DSD commented that in regard to certain activities it has sought legal advice on numerous occasions and 'has proceeded only where this advice has been unequivocal that the proposed activity was lawful'.[28] DSD commented that the Cybercrime Bill 'is an example of legislation, which without limited liability could have unintentionally restricted DSD's activities.'[29] ASIS stated:

> The Cybercrime Bill 2001 is an example of proposed legislation which has been drafted in response to global technological change and which includes provision for the legislation to have effect outside Australia. Without provision for limited liability under the bill ASIS could be restricted in its ability to achieve Government objectives.[30]

2.59 The IGIS confirmed the point that in recent times both ASIS and DSD were having to carefully review the legality of their operations. The IGIS stated:

> I have certainly come across instances where the legal regime we have in Australia as it relates to, potentially, activities overseas has

26 Australian Secret Intelligence Service, *Submission No. 3*, p. 5.
27 Australian Secret Intelligence Service, *Submission No. 3*, p. 5.
28 Defence Signals Directorate, *Submission No. 6*, p. 3.
29 Defence Signals Directorate, *Submission No. 6*, p. 3.
30 Australian Secret Intelligence Service, *Submission No. 3*, p. 5.

> caused them to think very carefully about, and in some cases to obtain legal advice about, the operations that they wish to conduct, where those operations, in my view as the Inspector-General, should cause no difficulty for us as Australians and for the agencies concerned.[31]

2.60 Both DSD and ASIS suggested that clause 14 was not unique and there are examples where immunity is provided under other Acts. For example, the Commonwealth Crimes Act provides for 'controlled operations' which gives 'federal law enforcement officers immunity from State drug possession offences, when certain pre-conditions are met.'[32] On the international front, the British *Intelligence Services Act 1994*, under section 7, provides for immunity to be granted for acts outside the British Islands.

2.61 ASIS indicated that for immunity to apply, there 'are clear and strict conditions that must be met' and, as such, 'there is no blanket immunity from Australian law.'[33] ASIS stated that for immunity 'to come into force the activity must:

- be preparatory to, or in support of, or otherwise directly connected with, overseas activities of ASIS; and
- involve aiding, planning or attempting to carry out or be directly connected with some other act outside Australia that would be an offence if committed within Australia; and
- be done in the proper performance of a function of ASIS.'[34]

2.62 The examination of clause 14 focused on the following three areas:

- the operation of clause 14;
- the accountability mechanisms; and
- terms and definitions.

Analysis – the operation of clause 14

2.63 During hearings, both DSD and ASIS were asked what steps they would take in the event that an activity they are undertaking, which is in breach of the law, was discovered by law enforcement officers. For example,

---

31 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 41.

32 Australian Secret Intelligence Service, *Submission No. 3*, p. 5, and Defence Signals Directorate, *Submission No. 6*, p. 3.

33 Australian Secret Intelligence Service, *Submission No. 3*, p. 5.

34 Australian Secret Intelligence Service, *Submission No. 3*, p. 5.

would the agencies seek to head the matter off as quickly as possible at the police investigation stage and prevent the activity from coming before a court.

2.64 DSD responded that it would go to the IGIS and seek advice.[35] The IGIS indicated that he would at some stage become involved. He indicated that he would expect that the proper level at which law enforcement authorities should be alerted is at Ministerial level. The IGIS concluded, however, that 'we should develop a protocol in case this kind of thing happens.'[36] DSD indicated that it would support the development of a protocol.[37]

2.65 ASIS explained the actions that would occur if an agent was discovered performing duties that were in breach of the law. The two types of transgressions include where an authorisation applies and where transgression is without authorisation.

2.66 ASIS indicated that where a report is made that a person, who is an ASIS officer, has broken the law, then the officer would need to alert the head of security of ASIS. ASIS would then 'get legal advice from the AGS and seek to bring in the government lawyer, who would then talk to the senior police in that jurisdiction to ensure that they knew what the circumstances were.'[38] At this point, ASIS would seek advice from the Australian Government Solicitor as to whether the officer was not breaking the law in terms of the IS Bill. If the action was consistent with the Bill then ASIS would seek approval for the action. If the officer's activity was not consistent with the Bill then ASIS would advise the Police to pursue their action against the officer. ASIS stated:

> If there was a consideration that the officer had broken the law then, in accordance with our current practices, we would advise that officer to seek legal advice and we would advise the police to pursue it, as they should. The basis of our approach to all of this is that an ASIS officer should be treated like any other Australian under Australian law. If the decision at that stage was to say, 'You have to go through with it,' our role through the use of the AGS would be to protect the Commonwealth's interests in that, which would be basically the name and the affiliation of the officer. If the police wanted to go ahead with the case, it would then go to the DPP. I imagine, at that stage, the AGS and a senior ASIS officer

35 Mr Ron Bonighton, Defence Signals Directorate , *Transcript*, p. 59.

36 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 61.

37 Mr Ron Bonighton, Defence Signals Directorate , *Transcript*, p. 61.

38 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 79.

> would fill the DPP in and the case would go to court. That is how that situation would progress under our current procedures. If, however, it was found that we thought he was within the law and the police were not convinced of that and wanted to go ahead, we would prepare a defence for that. But it would still go through the judicial processes.[39]

Conclusions

2.67 It became apparent during hearings that neither ASIS nor DSD had given careful consideration to the administration of clause 14 where an officer breaks the law and is discovered. If there is any abuse of clause 14 or a discoverable situation is administered with undue care then a serious controversy could arise that could lead to irreparable damage for the agencies and their use of clause 14.

2.68 It is essential, therefore, that protocols be developed to cover a range of scenarios regarding the application of clause 14. In particular, these protocols must provide lines of communication between the agencies and law enforcement agencies in each State and Territory. The agencies must include the IGIS in the development of the protocols.

2.69 We believe that the proposed Parliamentary Joint Committee on ASIO and ASIS should examine the protocols in its first year of operation as part of its responsibility to review administration and expenditure.

Recommendation 5

2.70 **The Director-General of ASIS, the Director of DSD and the Inspector-General of Intelligence and Security, in conjunction with the Australian Government Solicitor and relevant law enforcement agencies, in developing protocols for the operation of clause 14 of the Intelligence Services Bill 2001 and Division 476.5 of the Cybercrime Bill 2001, must ensure that:**

- **the protocols for the operation of clause 14 and Division 476.5 in respect of both ASIS and DSD be put in writing and approved by responsible ministers and the Attorney-General, and be provided as soon as possible to the IGIS;**
- **clause 14 and Division 476.5 should not come into effect until**

39 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, pp. 79-80.

the IGIS has received the protocols and the Parliamentary Joint Committee on ASIO and ASIS has been briefed on the protocols by IGIS; and

- **the Parliamentary Joint Committee on ASIO and ASIS should be briefed by the IGIS on the provisions of the protocols and any changes to the protocols.**

Analysis – accountability

2.71 One of the key accountability mechanism relating to clause 14 is the IGIS. He confirmed that 'the intention of the legislation as it is drafted in that area is not to give open slather to members of the agencies to break Australian law; it is simply to provide them with targeted immunity in cases where the operation of Australian law is such that it may cause difficulties for those kinds of operations.'[40] The IGIS indicated that he was not alarmed about clause 14 and stated:

> …given that my own office will, on a regular basis, be doing what it does: inspecting the operations of the agencies and ensuring that the capacity for the agencies to undertake these sorts of operations with that kind of immunity is not abused. I think it is fair to say that I have seen no instances of a desire on the part of the agencies to abuse their privileges in the past, and I have every reason to believe that they will not do so in the future. If I observed any instances of that, obviously I would take necessary action.[41]

2.72 The IGIS indicated that, in the course of his work, he is inspecting every current operation of ASIS. He stated that if 'there were activities going on in the course of those operations that were illegal or improper, I would have the power to act upon that knowledge.'[42] Overall, the IGIS indicated that the IS Bill improves his ability to do his job.[43] ASIS confirmed the role that the IGIS would have:

> Activities involving limited immunities will of course be subject to close scrutiny by the Inspector-General, as are all ASIS activities. The Inspector-General has access to all ASIS operational files and,

40 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 41.

41 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 41.

42 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 45.

43 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 47.

> as I have already noted, monitors the legality and propriety of ASIS activities.[44]

2.73 The Attorney-General for Victoria, the Hon Mr Rob Hulls, MP, stated that he was 'concerned that persons could commit offences in Victoria in pursuance of the functions of either ASIS or DSD without being subject to this State's criminal jurisdiction.'[45] Mr Hull suggested that there be stringent regulation regarding the immunity provisions. He proposed that 'potential breaches of the criminal law of the Commonwealth, State or Territories be specifically brought to the attention of the responsible Ministers when ASIS or DSD are seeking authorisations under clause 9 of the Bill.'[46] Mr Hulls concluded that 'such a requirement would ensure that such authorisations are given only after consideration of the full impact (including possible criminal activity) of the proposed activities.'[47]

2.74 ASIS indicated that in certain tasks, Ministerial authorisations provided under clause 9 will indicate that clause 14 will be invoked. In this way, this authorisation of tasking will act in a similar way to warrant provisions under the ASIO Act. However, ASIS indicated that not all ASIS activities, that rely on clause 14, could be linked to a ministerial authorisation under clause 9.

2.75 For example, if ASIS officers and other persons meet and discuss certain activities then they could be subject to conspiracy laws. In view of this, ASIS indicates that it would be impractical to seek a ministerial authorisation to talk and think about possible tasks and operations. ASIS states:

> Under clause 14(2) this limited liability extends beyond ASIS staff as there is a need to provide protection for those who assist ASIS and who task and authorise ASIS' activities. Under certain circumstances, without this protection, individuals including bureaucrats from departments and agencies and Ministers could find themselves in contravention of conspiracy provisions under various Australian laws.[48]

2.76 DSD indicated that, in their case, the granting of immunities would be closely linked to Ministerial authorisations and directions. DSD stated in relation to immunity provisions:

---

44 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 71.

45 Attorney-General for Victoria, *Submission No. 8* p. 1.

46 Attorney-General for Victoria, *Submission No. 8* p. 2.

47 Attorney-General for Victoria, *Submission No. 8* p. 2.

48 Australian Secret Intelligence Service, *Submission No. 3*, p. 5.

> Central to this is the question of ministerial authorisation and direction. We would want very clearly laid out for the minister, under that section of the bill, exactly what we propose to do over what time period. That has the effect of bringing the Inspector-General into the inspection procedure, because he has to check that what we have done matches those directions. In that ministerial authorisation, we would undertake to set out other sensitive areas that we might be involved in. That would be key to the operation of the legislation.[49]

2.77 During hearings, questions focused on whether ASIS conducts operations in Australia and, second, could the scenario arise where an ASIS officer or agent breaks an Australian law in an operational situation as opposed to a planning situation. This contingency is covered under subclause 14(2). ASIS argued that 14(2) did not provide an unlimited immunity to break Australian law. ASIS stated:

> If there is a need in the operation to break an Australian law, that must be agreed through the proper processes. It must be in terms of an activity that is clearly in accord with the limitations placed on that in the act. You cannot just go out onto the street and break the law and then claim immunity because you happen to be working with ASIS.[50]

2.78 ASIS was unequivocal that in an operational situation where an Australian law, other than a conspiracy provision, was required to be broken then ASIS would seek a Ministerial authorisation.[51] During this discussion, ASIS repeated that immunity could only be tied to the proper performance of its functions as set out in clause 6 and the limitations placed on it in clause 11. For example, if ASIS officers used violence in achieving their operations, then they could not seek immunity from prosecution 'because violence is specifically ruled out in the Bill as a limitation on our function.'[52] The Attorney-General's Department stated:

> It is not just the functions that we have to look at in terms of this immunity but the act as a whole and the other provisions and, as the director-general said, that relates to the prohibitions that are there. The act does not just say what can be done; it also says very specifically what cannot be done.[53]

---

49 Mr Ron Bonighton, Defence Signals Directorate , *Transcript*, p. 58 and 62.

50 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 75.

51 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 76.

52 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 77.

53 Mr Keith Holland, Attorney-General's Department, *Transcript*, p. 77.

2.79 ASIS sought to give reassurance that it would, through its planning, seek to identify if an Australian law would be broken and seek authorisation before the action. ASIS stated:

> If we anticipate anything that could break Australian law, we seek approval for it. If in the course of an operation something happens that was unexpected and it was thought to be against Australian law, we would seek to rectify that quickly. Once this act comes into place, we will have an education program going through ASIS to ensure that everyone understands precisely what the immunities, if they go through, mean and what they mean for them. If something were to happen and we learnt about it, we would immediately go to IGIS and seek to ensure that we did what was necessary then.[54]

2.80 In scrutinising clause 14, a range of scenarios were directed at ASIS in order to identify, if possible, any unintentional consequences of the immunity provisions. ASIS was asked if, under clause 14, it could break or enter or trespass. ASIS confirmed that, provided the correct authorisations were made, they could break and enter with immunity.[55] ASIS, however, in a supplementary submission of 7 August 2001, stated that it was not the 'intention of the agencies to obtain immunity for this type of activity.'[56]

2.81 The examination of ASIS regarding the break and enter scenario had, indeed, identified an unintentional consequence of clause 14. It was this matter which necessitated the Committee seeking leave from the Parliament to extend the reporting period to 27 August 2001. Further scrutiny of ASIS was required through a public hearing held on 20 August 2001. ASIS stated:

> Subsequent legal advice has confirmed that the immunities under Clause 14(2) could, as currently drafted, operate to confer immunity upon persons breaking and entering in Australia. Since receipt of that advice, the agencies have been working to find a formula which avoids that unintended result.[57]

2.82 ASIS confirmed that an activity such as breaking and entering 'would be conducted at the request of the relevant Minister under ASIO warrant in

54 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, pp. 78-79.

55 Mr Keith Holland, Attorney-General's Department, *Transcript*, p. 81.

56 Australian Secret Intelligence Service, *Submission No. 17*, p. 1.

57 Australian Secret Intelligence Service, *Submission No. 18*, p. 2.

accordance with the *Australian Security Intelligence Organisation Act 1979*.'[58] ASIS stated that this procedure 'will remain the legal requirement.'[59]

2.83 ASIS' proposal to remove the unintended consequence identified by the Committee is the 'deletion of the current subclause (2)(b)(ii) of clause 14 in its entirety, making an addition to the existing subclause (2)(b)(i) and clarifying the intentions of the agencies in the Explanatory Memorandum. Clause 14, with the proposed ASIS amendments, is produced in full below:

14 Liability for certain acts

(1) A staff member or agent of an agency is not subject to any civil or criminal liability for any act done outside Australia if the act is done in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for any act done inside Australia if:

(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and

(b) the ~~act:~~

~~(i) involves~~ act involves aiding, abetting, counselling, procuring or otherwise planning, or carrying out or attempting to carry ~~out; or~~

~~(ii) is otherwise directly connected with;~~

~~some~~ out some other act outside Australia that would amount to an offence if that other act were committed in Australia; and

(c) the act is done in the proper performance of a function of the agency.

(3) In this section:

***act** includes omission.*

***staff member** includes the Director and the Director-General.*

2.84 ASIS indicated that the proposed amendments to clause 14 'will narrow the scope of the immunity by excluding acts which do not have such a close connection as that required by subclause (b)(i).'[60] In particular, ASIS emphasise that paragraphs 14(2) (a) and (c) 'make it clear that any act

58 Australian Secret Intelligence Service, *Submission No. 18*, p. 2.

59 Australian Secret Intelligence Service, *Submission No. 18*, p. 2.

60 Australian Secret Intelligence Service, *Submission No. 18*, p. 2.

which was outside the agencies' specific statutory functions would not be covered by the immunity.'[61] ASIS stated:

> For instance sub-clause 6(4) makes it clear that ASIS is not permitted to engage in acts of violence and clause 7 in setting out the functions of DSD makes clear that its functions in relation to the gathering of intelligence are directed towards people or organisations outside Australia. It is also necessary to have regard to the other limitations embodied in the Bill such as clauses 11 and 12. The functions of each agency are quite specific in focussing their activities outside Australia.[62]

2.85 The Office of Parliamentary Counsel (OPC) confirmed that, in applying subclause 14(2), 'you need to look at what the limitations are on the proper performance of the functions.'[63] The OPC commented that these limitations are in other parts of the Bill 'starting from 6 and 7 and working through also 11 and 12.' OPC confirmed that these clauses are central to the operation of paragraph 14(2)(c). If 14(2)(c) is not satisfied then the immunity under 14(2) is not available.[64] The OPC stated:

> What I can say is that I am satisfied that the only acts for which there is immunity under 14(2) are those which can somehow be brought within the description of the proper performance of a function of the agency, and that the effect of these function provisions will be to exclude a lot of the sorts of activities that I think are concerning you. But I could not say that it will exclude everything that could possibly be an offence under Australian law, somehow.[65]

2.86 The OPC also confirmed that clause 14, subject to the proposed amendments, would not enable DSD to intercept telecommunications in Australia, and nor would it enable ASIS to conduct covert operations in Australia involving listening devices, search and enter, remotely accessing data in a computer, use of tracking devices, and mail interception.[66] Although, OPC commented that while '14(2) is not really ambiguous', 'the exact boundaries are not readily identifiable.'[67]

2.87 ASIS indicated that the immunity provisions are intended to deal with:

61 Australian Secret Intelligence Service, *Submission No. 18*, p. 2.
62 Australian Secret Intelligence Service, *Submission No. 18*, p. 2.
63 Ms Hilary Penfold, Office of Parliamentary Counsel, *Transcript*, p. 114.
64 Ms Hilary Penfold, Office of Parliamentary Counsel, *Transcript*, p. 114.
65 Ms Hilary Penfold, Office of Parliamentary Counsel, *Transcript*, p. 115.
66 Ms Hilary Penfold, Office of Parliamentary Counsel, *Transcript*, p. 117.
67 Ms Hilary Penfold, Office of Parliamentary Counsel, *Transcript*, pp. 121-122.

- conspiracy;
- extra-territoriality (the extra territorial effect of some Australian laws);
- the territorial nexus provisions in some law – ie the linkage between some Australian law and acts or events in another jurisdiction; and
- agencies acting in Australia as part of a continuous activity focussed on foreign intelligence collection overseas.[68]

2.88 The proposal was made during hearings that the immunity provisions in clause 14 should reflect what is identified in the previous dot points. The OPC suggested that clause 14 could be amended to more closely reflect the list of issues above but 'you would very quickly find that what you came up with just had its own set of problems about where the boundaries lay.'[69] For example, OPC stated in relation to dot point four above:

> …'continuous activity' is another one of those words where you may be able to say, 'I know it when I see it,' but you certainly cannot say, 'This is exactly where the boundary lies. That falls outside; that falls inside.' I am not convinced that we would really overcome the problem that you are seeing, which is that at the moment none of us really know exactly some of the things that might need to be covered, but we rely on the limitations of the proper performance of functions.[70]

2.89 Notwithstanding these concerns, OPC provided an alternative formulation for paragraph 14(2)(b) which is reproduced, in full, below:

> *(b) the act:*
>
> *(i) taken together with an act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but*
>
> *(ii) in the absence of that other act, event, circumstance or result, would not amount to an offence; and*[71]

2.90 In addition, OPC suggested that the correct interpretation of the provision set out above would be furthered by the inclusion in the EM of paragraphs along the following lines:

---

68 Australian Secret Intelligence Service, *Submission No. 18*, p. 1.

69 Ms Hilary Penfold, Office of Parliamentary Counsel, *Transcript*, p. 122.

70 Ms Hilary Penfold, Office of Parliamentary Counsel, *Transcript*, p. 122.

71 Office of Parliamentary Counsel, *Submission No. 21*, p. 1.

> The agencies should not be given immunity in respect of civil and criminal liability for acts against Australian law committed wholly within Australia and without foreign elements. However it is considered that, in Australia's interests, agencies should have immunity in respect of certain acts in Australia that are connected with activity outside Australia, even where those acts might give rise to liability under an Australian law, if the liability only arises in the particular case because the Australian law has an aspect of extra-territorial application.
>
> Paragraph 14(2)(b) therefore applies to an act that forms a part of an offence under Australian law, but only where, in the particular case, at least one of the parts of that offence was an act, event, circumstance or result that took place, or was intended or expected to take place, outside Australia. Thus, the paragraph only applies to an act done in Australia:
>
> - where that act, taken together with an act, event, circumstance or result that took place, or was intended or expected to take place, outside Australia, could amount to an offence, and
> - where that act, in the absence of the other act, event, circumstance or result, would not amount to an offence.[72]

2.91 The IGIS confirmed that the proposed amendments by OPC would be effective. The IGIS suggested that the amendment that is proposed to the original formulation makes it abundantly clear that the only actions that would be attracting this immunity would be those that were directly connected with the proposed overseas operation.

2.92 During the final public hearing, ASIS was scrutinised on the extent to which subclause 14(1) would allow ASIS to gather intelligence on an Australian citizen or organisation based overseas. ASIS, in the first instance, commented that it does 'not set out to collect intelligence on Australian citizens–that is not the intention of the organisation.'[73] Following further questioning, it became clear that the Bill does provide ASIS with the power to collect intelligence on Australians overseas. ASIS stated:

> We are empowered to collect intelligence on the capabilities and so on. If an Australian, for example, were an agent of a foreign power then that would come within the terms of it. It does not rule out

72 Office of Parliamentary Counsel, *Submission No. 21*, p. 2.

73 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 96.

> Australians—I suppose that is the fact—but it defines how they come into our collection processes.[74]

2.93 ASIS pointed out that there are nationality rules, currently operating, and the provision of privacy rules under clause 15 of the IS Bill which seek to protect the privacy of Australians overseas.[75] ASIS commented that there 'are strict categories under which we would have Australians in our reports, and they are limited to issues like national security, and the protection of Australian lives'.[76] ASIS confirmed that provided there were significant reasons then it could for example undertake covert entry to premises, undertake searches, and use listening and tracking devices against Australian citizens living overseas.[77]

2.94 ASIS were asked whether the ASIO warrant system had been considered as a possible system for ensuring accountability in those instances where an Australia living overseas was targeted. ASIS stated:

> …yes, it has been looked at and not found to be particularly practicable because of the nature of the immunities that we are seeking—that is, narrow immunities relating to the extraterritorial application of Australian law or the territorial nexus. To seek a warrant for activities overseas which might bring the need for those immunities into play would be particularly difficult given the nature of a warrant, which, as I understand it, is for something specific for a particular time.[78]

2.95 ASIS confirmed, through questioning, that if, for example, the property of an Australian citizen living overseas was damaged as a result of an ASIS activity then the Australian citizen would have no recourse through Australian courts.[79] The purpose of raising hypothetical situations, during the hearings, was to test the limits of the legislation. The IGIS commented, however, that he had 'never seen anything remotely approaching' the types of hypotheticals which were raised.[80]

---

74 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 96.
75 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 96.
76 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 96.
77 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 97.
78 Mr Alan Taylor, Director-General, Australian Secret Intelligence Service, *Transcript*, p. 97.
79 Mr Stephen Marshall, Australian Security Intelligence Organisation, *Transcript*, p. 102.
80 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 104.

Conclusions

2.96 The objective in examining clause 14 was to ensure that the administration of the immunity provisions could not be abused in any way, and there were no unintended consequences of the provision.

2.97 During hearings, a range of scenarios were directed at ASIS to test the operation of clause 14. One scenario focused on the possibility that clause 14 could give ASIS immunity to break and enter. ASIS confirmed that this was the case and in doing so confirmed an unintended consequence of clause 14. ASIS subsequently proposed an amendment to subclause 14(2) which would remove the unintended consequences identified.

2.98 We consider the problems identified with subclause 14(2) significant. The proposed amendments to 14(2) were examined in detail through an additional hearing. ASIS, under the proposed amendments to clause 14, will have no immunity to conduct an activity such as break and enter. The offending subparagraph 14(2)(b)(ii), 'is otherwise directly connected with' is deleted under the amendment.

2.99 ASIS will only receive immunity for acts which are set out in ASIS functions under clause 6 and governed through limitations in clauses 11 and 12 which place limits on agencies functions and activities. For example, under subclause 6(4) ASIS must not plan for, or undertake, paramilitary activities or activities involving violence against the person or the use of weapons.' In relation to DSD, under clause 7, it can only obtain intelligence about people or organisations outside Australia.

2.100 The proposed OPC amendments to paragraph 14(2)(b) are a further enhancement to the overall operation of clause 14. In addition, the changes to the EM proposed by the OPC help to ensure a correct interpretation of the clause. In view of this, the Committee supports the amendments to paragraph 14(2)(b) proposed by the OPC.

2.101 Provided that the OPC amendments to subclause14(2) are made and the EM is amended then we support clause 14.

2.102 The amendments will ensure that clause 14 serves the purpose for which it was intended. In addition, the proposed Parliamentary Committee on ASIO and ASIS should, on an annual basis, review the generality of the administration of clause 14 and report its findings to the Parliament.

Recommendation 6

2.103 **Subclause 14(2) of the Intelligence Services Bill 2001 be amended to read:**

- **(2) A person is not subject to any civil or criminal liability for any act done inside Australia if:**
  - ⇒ **(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and**
  - ⇒ **(b) the act:**
    - ⇒ **(i) taken together with an act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but**
    - ⇒ **(ii) in the absence of that other act, event, circumstance or result, would not amount to an offence; and**
  - ⇒ **(c) the act is done in the proper performance of a function of the agency.**

In addition, a new subclause 2A be added to clause 14 that would read:

- **(2A) Subsection (2) is not intended to permit any act in relation to premises, persons, computers, things, or telecommunications services in Australia, being an act that ASIO could not do without a Minister authorising it by warrant issued under Division 2 of Part III of the Australian Security Intelligence Organisation Act 1979 or under Part III of the Telecommunications (Interception) Act 1979 or an act to obtain information that ASIO could not obtain other than in accordance with section 283 of the Telecommunications Act 1997.**

Division 476.5, paragraph 2 of the Cybercrime Bill 2001 be amended to reflect the amendments proposed for subclause 14(2) of the Intelligence Services Bill 2001.

2.104 The key accountability mechanisms relating to the operation of clause 14 involve the Inspector-General of Intelligence and Security (IGIS), and the use of Ministerial authorisations. The IGIS has oversight of all ASIS operational files. In addition, all Ministerial authorisations issued under clause 9 are automatically provided to the IGIS.

2.105 A proposal was made by the Victorian Attorney-General that all cases where the law is broken should be alerted through a Ministerial authorisation under clause 9. DSD advised that this will occur for all operations which may break the law and therefore clause 14 is invoked. ASIS also indicated that, for all operational activities that may break the law, then a Ministerial authorisation under clause 9 would be sought.

2.106 ASIS, however, indicated that it would not be practical to seek a Ministerial authorisation for activities involving planning and discussion of operations which may be subject to conspiracy laws. The same situation applies to DSD.

2.107 While it is not reasonable to expect ASIS or DSD to seek Ministerial authorisation for all planning activities, we believe it is essential that the agencies seek prior Ministerial authorisations under Clause 9 for all operational activities that may break the law.

2.108 The proposed Parliamentary Joint Committee on ASIO and ASIS should seek advice, on an annual basis, from the IGIS on the volume of Ministerial authorisations issued under clause 9 which refer to potential claims for immunity under clause 14.

Intelligence collection on Australians overseas

2.109 Clauses 6 and 7 of the Bill empower ASIS and DSD to obtain information in respect of foreign persons and organisations overseas *and Australian persons and organisations overseas*. The Bill makes no distinction between persons or organisations on the basis of nationality other than in the provisions of clause 15 relating to privacy rules.

2.110 During the final public hearing, a range of hypothetical situations were directed at ASIS in relation to its powers to gather intelligence on Australians citizens or organisations based overseas.

2.111 In evidence to the Committee, both ASIS and DSD emphasised that in the normal course of operations neither agency targets Australian citizens overseas for intelligence collection. Both agencies stated their purpose is 'foreign intelligence' collection, though this term is *not* used in the Bill. Both ASIS and DSD did acknowledge, however, that in certain limited circumstances (i.e. a matter of national security) it could be appropriate and permissible under current practice to collect intelligence concerning an Australian citizen or organisation overseas. These circumstances are not specifically identified or defined in the Bill.

2.112 While ASIS and DSD gave assurances that they do not target Australians, it is how the legislation is interpreted and used in five, ten or twenty

years time that concerns this Committee. When a Parliament passes legislation, it is not the assurances of individual officers that matter, it is how legislation is interpreted and can potentially be used that is of consequence. Whatever is current practice or intentions, the Bill will establish a new legal reality within which future decisions about possible ASIS and DSD operations will be made.

2.113 Subclause 14(1) provides ASIS and DSD with immunity from civil or criminal liability for any act done outside Australia in the proper performance of their intelligence gathering functions.

2.114 The Committee believes that there are insufficient accountability mechanisms governing the authorisation of ASIS and DSD intelligence collection concerning Australian persons or organisations overseas. Accordingly, the IS Bill requires amendment to include a special authorisation process for any activities specifically directed towards obtaining intelligence concerning Australian persons or Australian organisations overseas. This authorisation process must ensure that any intelligence collection activities specifically directed towards Australian citizens or Australian organisations overseas must relate to questions of national security.

2.115 The authorisation process proposed by the Committee will require amendment to clauses 8 and 9. The following recommendation will narrow the scope of possible intelligence collection directed towards Australian persons or Australian organisations to matters of national security and introduce an authorisation regime comparable with the provisions of Division 2 (Special Powers) of the *ASIO Act 1979*.

2.116 In view of the fact that ASIS and DSD have confirmed that they do not set out to collect intelligence on Australians overseas except in limited circumstances relating to national security, then they should have no objection to this requirement. We assert that this is a threshold requirement with which ASIS and DSD must comply.

2.117 It should be noted that the term ‘national security’ which is referred to in clause 11 and in the following recommendation is not defined in the Bill. The IS Bill should be amended to include a definition of ‘national security’. In addition, the IS Bill does not include a definition of ‘Australian organisations’. A recommendation proposing that these terms be defined in the IS Bill is included in Chapter 4.

Recommendation 7

2.118 **Clauses 8 and 9 of the Intelligence Services Bill 2001 be amended to require authorisation by the responsible Minister for any activity specifically directed towards obtaining intelligence concerning Australian persons or Australian organisations overseas, and**

- **that in giving any such authorisation under clause 9 the Minister must be satisfied that the Australian person or organisation overseas is engaged in, or is reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to Australia's national security;**
- **that the activity proposed to be authorised be likely to assist the obtaining of intelligence relevant to national security;**
- **that any such authorisation have effect for six months, whereupon it will lapse unless renewed by the Minister.**

Analysis – terms and definitions

2.119 Subclause 14(2) brings attention to the use of certain terms and their definitions. Subclause 14(1) refers to 'a staff member or agent of an agency'. Subclause 14(2) states that 'a *person* is not subject to…'. The use of the word 'person' in 14(2) was the focus of examination during hearings.

2.120 The IS Bill and its EM do not provide a definition of 'person'. There was some concern that its use could lead to a range of unspecified people acquiring immunity. ASIS responds that the term 'person' in 14(2) is deliberate and covers all those persons, including the Minister, that could be involved in discussions regarding planning for tasks or operations which could be a contravention of conspiracy provisions. The Attorney-General's Department states:

> In addition to agency staff members and agents, those persons intended to be covered include those who task and direct ASIS or DSD such as the responsible Minister, the members of the National Security Committee of Cabinet, senior officers within Departments and agencies, or those who may have particular technical or other knowledge, expertise or capabilities that could assist ASIS or DSD to plan and conduct an operation overseas.[81]

81 Attorney-General's Department, *Submission No. 15*, p. 2.

2.121 In view of the possibility that a range of persons could be involved with ASIS when it is planning its tasks and operations, ASIS concluded that it is problematic to include a definition that would cover those people who would constitute being a 'person' under 14(2).

2.122 The ASIO Act makes reference to 'people' in subsection 24(1) – Exercise of authority under warrants etc. Section 24 states that the 'Director-General, or a senior officer of the Organisation appointed by the Director-General in writing to be an authorising officer for the purposes of this subsection, may, by signed writing, approve officers and employees of the Organisation, and *any other people*, as people authorised to exercise, on behalf of the Organisation, the authority conferred by relevant warrants or relevant device recovery provisions.'

2.123 Subsection 24(1) of the ASIO Act provides for authorised people to conduct activities under warrant. ASIS and DSD, as previously discussed, have indicated that they may not always be able to seek authorisation for activities involving planning. ASIS states:

> Given the extra-territorial effect of some Australian law (eg conspiracy provisions and territorial nexus provisions) these persons, depending on the nature and circumstances of the operation, could be committing an offence under Australian law, by virtue of their, albeit limited, involvement in Australia in directing, approving, tasking or assisting in relation to an ASIS or DSD operation overseas. The 'person' assisting the agency may vary depending upon the type of operation being considered and the knowledge and expertise required to assist in either planning or carrying out the operation.[82]

2.124 In order to clarify the use of 'person' in subclause 14(2), ASIS consulted with the Attorney-General's Department and the Office of Parliamentary Counsel. The objective was to establish an 'independent mechanism to identify more precisely which person and activities may be subject to the immunities conferred under clause 14.'[83]

2.125 The agencies examined the approaches used in other Commonwealth legislation to confer specific types of immunity under Australian law. These Acts include section 15U of the *Crimes Act 1914*, section 14 of the *Consular Privileges and Immunity Act 1972*, and section 18 of the *Defence (Visiting Forces) Act 1963*. ASIS noted that these 'statutes all include a specific provision under which an appropriate authority may certify facts

82 Australian Secret Intelligence Service, *Submission No. 18*, p. 3.

83 Australian Secret Intelligence Service, *Submission No. 18*, p. 3.

which may be relevant to the determination of immunity for the purposes of the legislation, and such certificates are made admissible in proceedings within Australia.'[84] ASIS stated:

> It would be possible to adopt a similar approach in order to clarify the possible existence of immunity under clause 14 of the Intelligence Services Bill. For example, clause 14 could include an additional paragraph which enables the Inspector-General of Intelligence and Security to give a certificate in writing certifying any fact relevant to the question of whether an act done inside Australia was done in the proper performance of a function of the agency concerned.[85]

2.126 ASIS proposed that clause 14 be amended by adding the following paragraphs:

- The Inspector-General of Intelligence and Security may give a certificate in writing certifying any fact relevant to the question of whether an act done inside Australia was done in the proper performance of a function of an agency.
- In any proceedings, a certificate given under subsection (above) is prima facie evidence of the facts certified.[86]

2.127 The effect of these paragraphs, if inserted into clause 14, would ensure that any *person* claiming immunity would need a certificate provided by the IGIS. ASIS indicated that the role of the IGIS in performing this function would be consistent with the existing functions of the Inspector-General under *Inspector-General of Intelligence and Security Act 1986*.

2.128 ASIS also proposed that the Explanatory Memorandum be revised to reflect the role of the IGIS and the new accountability mechanism.

2.129 The IGIS commented that his role in certifying certain acts 'would provide a safeguard that the public could be confident would be adequate.'[87]

2.130 The OPC confirmed that it would be possible to construct a provision in the IS Bill to reflect the additional lines which involve the IGIS in the operation of clause 14.[88]

---

84 Australian Secret Intelligence Service, *Submission No. 18*, p. 3.

85 Australian Secret Intelligence Service, *Submission No. 18*, pp. 3-4.

86 Australian Secret Intelligence Service, *Submission No. 18*, p. 4.

87 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, p. 95

88 Ms Hilary Penfold, Office of Parliamentary Counsel, *Transcript*, p. 122.

Conclusions

2.131 The use of the word 'person', in subclause 14(2), which is not defined was, in the first instance, a concern for the Committee. Anyone reading *person* in 14(2) may interpret that a range of unspecified people could claim immunity under clause 14.

2.132 The use of the word 'person' in 14(2) was rigorously examined during hearings. ASIS' initial response was based on the variety of people, including the Minister, that could be involved in activities involving planning which may be subject to conspiracy laws. We did not consider that this was sufficient reasoning for the use of 'person' in 14(2) in the absence of any accountability mechanisms. Clause 14, in its original form, provides no assurance that a range of unspecified persons could claim immunity.

2.133 ASIS responded to our concerns by consulting with the Attorney-General's Department and the Office of Parliamentary Counsel in developing an accountability mechanism that will involve the Inspector-General of Intelligence and Security (IGIS). The IGIS has also been consulted on and supports the proposed accountability mechanism. Under this system, the IGIS may give a certificate in writing certifying any fact relevant to the question of whether an act done inside Australia was done in the proper performance of a function of an agency. What this means is that any 'person' who claims immunity under clause 14 would need a certificate from the IGIS verifying that they had carried out an activity which was done in the proper performance of a function of an agency.

2.134 The use of the word 'person' in subclause 14(2) was an initial concern. However, we believe that our scrutiny of 14(2) has helped produce a solution which provides accountability and confidence. Provided the following additions are made to clause 14, and the EM is revised then we support the version of clause 14 as revised by recommendation 6 above.

Recommendation 8

2.135 **The following subclauses be added to clause 14 of the Intelligence Services Bill 2001:**

- **The Inspector-General of Intelligence and Security may give a certificate in writing certifying any fact relevant to the question of whether an act was done in the proper performance of a function of an agency.**
- **In any proceedings, a certificate given under subsection (above) is prima facie evidence of the facts certified.**

Clause 15 – Rules to protect privacy of Australians

2.136 Clause 15 provides a framework for protecting the privacy of Australians in relation to the work performed by ASIS and DSD. The EM states that the 'agencies are required to take all possible measures to ensure that their activities are undertaken with due regard to the rights of Australians to privacy.' In achieving this objective the responsible Minister must make written rules regarding communication and retention by agencies of intelligence information concerning Australians. In making the rules, the Minister must consult with the IGIS. In addition, the IGIS also monitors compliance with the rules.

2.137 Clause 15 is produced, in full, below:

15 Rules to protect privacy of Australians

(1) The responsible Minister in relation to ASIS, and the responsible Minister in relation to DSD, must make written rules regulating the communication and retention by the relevant agency of intelligence information concerning Australian persons.

(2) In making the rules, the Minister must have regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by the agencies of their functions.

*Note: For **Australian person** see section 3.*

(3) Before making the rules, the Minister must consult with:

(a) in the case of ASIS—the Director-General; and

(b) in the case of DSD—the Director; and

(c) in either case—the Inspector-General of Intelligence and Security.

(4) For the purpose of consultations under paragraph (3)(c), the Minister must provide a copy of the rules the Minister is proposing to make to the Inspector-General of Intelligence and Security.

(5) The agencies must not communicate intelligence information concerning Australian persons, except in accordance with the rules.

*Note: For **intelligence information** see section 3.*

Analysis

2.138 The IGIS commented that the privacy framework provided through clause 15 is robust. The IGIS stated:

> The rules that would be made under this legislation would be basically the same as the rules that are already in existence. I think there is scope for some tidying up and improvement of the rules because, inevitably with these kinds of things, you come across circumstances that mean that you need to make adjustments to them as time goes on. But I think that the rules are fundamentally sound and having them regulated by virtue of this legislation I think would be a good thing. The regime that the legislation provides for privacy is a robust one. I believe too that having it regulated in the way that it will be regulated provides further insurance against abuse of the privacy rights of Australians.[89]

2.139 The ACCL had reservations because the proposed Parliamentary Committee under the Bill would not be able to review the privacy rules. The ACCL stated:

> The weakness of the Committee's supervisory role is reflected in Section 29(3)(f), which indicates the functions of the Committee do not include reviewing the privacy rules made by the Minister regulating the communication and retention by ASIS or DSD of information concerning Australian citizens.[90]

89 Mr Bill Blick, Inspector-General of Intelligence and Security, *Transcript*, pp. 41-42.

90 Mr Terry O'Gorman, Australian Council for Civil Liberties, *Transcript*, p. 39.

Conclusions

2.140 We are satisfied that the privacy regime provided for under clause 15 is satisfactory. It is noted that the IGIS commented that 'there is scope for some tidying up and improvement of the rules'. The Minister, in developing the privacy rules under 15(1), should note the appraisal by IGIS that the existing rules can be enhanced.

2.141 It is noted that the proposed Parliamentary Committee will not be able to, under paragraph 29(3)(f), review the privacy rules made under clause 15. We, however, suggest that the proposed Parliamentary Committee will be able to have indirect input into the privacy rules through its power to call and cross-examine the IGIS. The IS Bill should be amended to reflect this process.

Recommendation 9

2.142 **A new subclause be added to clause 15 of the Intelligence Services Bill 2001 to require that the Parliamentary Joint Committee on ASIO and ASIS be briefed by the IGIS on the privacy rules and any changes to their provisions.**