

# CHAPTER 3

## KEY ISSUES

3.1 The committee received submissions from a range of organisations and individuals for this inquiry. Submissions from the Queensland Police Service and the Law Society of Western Australia expressed broad support for the Bill.<sup>1</sup> The New South Wales Minister for Police and Emergency Services also offered support for the Bill, advising that the proposed amendments do not raise any specific legal issues for the NSW Police Force and that the Bill appears uncontentious from a law enforcement point of view.<sup>2</sup>

3.2 However, a number of submissions received by the committee raised concerns with Items 3, 7 and 13 of Schedule 1 of the Bill, which relate to ASIO's power to collect foreign intelligence. Other aspects of the Bill which the committee received comment on were Item 4, which amends the ASIO Act to clarify that computer access warrants authorise ongoing access to the relevant computer during the life of the warrant; and Items 19 and 26, which amend certain immunity provisions in the IS Act and the Criminal Code to clarify that those provisions can only be overridden by express legislative intent.

### **Collection of foreign intelligence under the ASIO Act**

3.3 As noted above, concerns were raised about the proposed amendments contained in Items 3, 7 and 13 of Schedule 1 of the Bill which will amend certain provisions of the ASIO Act dealing with ASIO's power to collect foreign intelligence. Those items expand the definition of 'foreign intelligence', along with the scope of provisions relating to foreign intelligence collection warrants and authorisations.

3.4 The Law Council of Australia (Law Council) expressed its opposition, not only to the breadth of the proposed new definition of 'foreign intelligence', but also to the amended test in sections 27A and 27B. It recommended that Items 3, 7 and 13 be removed from the Bill.<sup>3</sup>

3.5 At the public hearing, Ms Rosemary Budavari articulated the Law Council's position:

The Law Council opposes the proposed amendments relating to the definition of foreign intelligence essentially for two reasons. The first reason is that we consider that no real case has been made out to justify them, and certainly not one which takes proper account of the full scope of

---

1 See *Submission 5* and *Submission 10*.

2 *Submission 7*, p. 1.

3 *Submission 1*, p. 3.

ASIO's existing powers and which explains by reference to more than fairly broad statements why those powers are inadequate. In this context it is important to note ASIO's existing powers to gather information that are relevant to security and the fairly broad definition of security that is already within the Act. The materials that support this bill, the explanatory memorandum and submissions in our respectful submission from the Attorney-General's Department, do not clearly spell out the effect of the amendments nor provide sufficient justification for them. For example, what is not clearly stated is that the amendments are not simply about allowing ASIO to do the same work it has always done—for example, counterterrorism work, but in a different threat environment which is referred to in those materials—but, in fact, potentially allow ASIO to do different work altogether—for example, gathering information about economic activity and negotiations. In short, the amendments expand ASIO's sphere of activity.<sup>4</sup>

3.6 Ms Budavari continued:

The second reason that we oppose the new proposed definition and the threshold test for the authorisation of the gathering of this foreign intelligence is that these provisions are so broadly drafted they no longer fulfil their purpose. They do not simply substitute new parameters for old parameters, but they replace statutory parameters with broad ministerial discretion and that starts to undermine the purpose and effectiveness of the act. In this regard we contrast the test for the use of these powers with the threshold test for ASIO gathering information in relation to domestic matters which is far more tightly defined.<sup>5</sup>

3.7 While acknowledging the changing nature of threats to Australia's security,<sup>6</sup> the Law Council described the proposed changes as affording 'the Minister and [ASIO] almost unfettered discretion to determine when and how ASIO's powers may be used to gather information about people's activities, communication and relationships abroad.'<sup>7</sup> The Law Council outlined the impact of the proposed amendments in Items 3, 7 and 13:

[T]he proposed amendments to the definition of "foreign intelligence", coupled with the further proposed amendment to the test in sections 27A and 27B, will mean that search warrants, computer access warrants and surveillance and listening device warrants are available to ASIO in a very broad range of circumstances. The proposed changes will almost render meaningless the threshold test that must be met by ASIO in order to obtain a warrant or authorisation to collect intelligence under 27A and 27B. A warrant or authorisation will be able to be obtained to gather information about the activities of *any* person or group outside Australia whenever those

---

4 *Committee Hansard*, 16 June 2011, p. 1.

5 *Committee Hansard*, 16 June 2011, p. 2.

6 *Supplementary Submission*, p. 2.

7 *Submission 1*, p. 2.

activities are considered to be somehow relevant to Australia's national security, Australia's foreign, relations or Australia's economic well-being.<sup>8</sup>

3.8 The Castan Centre for Human Rights Law (Castan Centre) was also critical of the proposed broadening of the definition of 'foreign intelligence' and the amended conditions for the issue of foreign intelligence warrants under the Bill. It also recommended that Items 3 and 7 should not be enacted unless more detailed reasons can be given as to why ASIO's capabilities need to be expanded in the ways for which those items provide.<sup>9</sup>

3.9 The Castan Centre argued that the current definition of 'foreign intelligence', which includes 'a foreign political organisation', adequately covers most non-state organisations that may threaten national security:

[B]oth individuals and organisations that are linked to threats or acts of politically-motivated violence, even if the violence has nothing to do with Australia, would fall under the current definition of security, which includes all offences again Part 5.3 of the *Criminal Code* (Cth), meaning that ordinary special powers warrants would be available in respect of them.<sup>10</sup>

3.10 The Castan Centre agreed that the amendments would allow ASIO a wider scope to investigate the activities of Australians who are overseas, whose activities do not pose a threat to Australia's security but do have implications for Australia's foreign relations or economic interests.<sup>11</sup> Two examples were presented in that regard:

An example of such activities might include the release of secret government information by an Australian living abroad, such as has been the case in respect of Julian Assange and Wikileaks. Currently, information about Wikileaks probably would not constitute foreign intelligence – because Wikileaks is (arguably) not a foreign political organisation, and its activities do not threaten Australia's security (as defined in section 4 of the *Australian Security Intelligence Organisation Act 1979* (Cth)). But Wikileaks is an organisation, and Mr Assange is a person, outside Australia, and their activities evidently do have implications for Australia's foreign relations. This example shows how the notion of "person or organisation outside Australia", combined with the notion of "Australia's foreign relations", very considerably expands the scope of ASIO's potential activities.

Another example can be given by combining the notion of "intelligence pertaining to organisations outside Australia" with the notion of "Australia's national economic wellbeing". This suggests that the amendments would permit ASIO to engage in certain forms of economic or industrial

---

8 *Submission 1*, p. 2.

9 *Submission 2*, p. 4.

10 *Submission 2*, pp 2-3

11 *Submission 2*, p. 3.

espionage, including in relation to Australians working for overseas firms that are major rivals to key Australian industries.<sup>12</sup>

3.11 The Federation of Community Legal Centres Victoria also voiced concern about the expansionary implications of the proposed amendments under Item 3 and 7 of Schedule 1 of the Bill, and endorsed the Castan Centre's submission.<sup>13</sup>

### ***Departmental response***

3.12 The Attorney-General's Department (Department) explained that the rationale for the proposed changes relating to the definition and collection of foreign intelligence under the ASIO Act is to align it with the IS Act and the TIA Act. The Department further advised that the amendment will result in a consistent approach to foreign intelligence collection and authorisations, enhancing interoperability and intelligence sharing and allowing for more efficient processes for collecting and communicating foreign intelligence.<sup>14</sup>

3.13 In addressing concerns about the breadth of the proposed amendments, the Department emphasised the importance of aligning ASIO's foreign intelligence collection with that of other relevant intelligence agencies, to ensure a complementary role and to eliminate potential gaps in intelligence coverage.<sup>15</sup> However, the Department assured the committee that '[t]his is not 'consistency for the sake of consistency' – rather it reflects that ASIO has long played a role that is intended to complement the foreign intelligence role of the other intelligence agencies' and that those roles 'have not been completely aligned because legislation was drafted at different times, reflecting different threat environments'.<sup>16</sup>

3.14 With respect to specific concerns about a possible lowering of the threshold test for the collection of foreign intelligence, the Department reiterated that 'this is already the construct within which Australia's foreign intelligence agencies collect foreign intelligence and which sets the three broad boundaries which have been enshrined in the [IS] Act since 2001. This definition has provided the parameter for the activities of Australia's foreign intelligence collection agencies (ASIS, DSD, DIGO) since their creation'.<sup>17</sup> The Department advised that it did not expect 'that this amendment will result in significantly more foreign intelligence collection warrants or authorisations being issued under the ASIO Act';<sup>18</sup> and that ASIO's core focus will

---

12 *Submission 2*, pp 3-4.

13 *Submission 3*, p. 2.

14 *Submission 4*, p. 1.

15 *Submission 4*, p. 2.

16 *Second Supplementary Submission*, p. 5.

17 *Second Supplementary Submission*, p. 6.

18 *Second Supplementary Submission*, p. 5.

continue to be its security intelligence function, as opposed to the collection of foreign intelligence.<sup>19</sup>

### 3.15 Further:

The proposed amendment does not create a broad new power or space for ASIO to engage in new activities or 'economic espionage'. It merely seeks to apply the existing parameters already applicable to foreign powers and political organisations to individual 'non-state' actors as part of the harmonisation of the legislative definitions. This is designed to facilitate more streamlined cooperation between ASIO and the foreign intelligence agencies and minimise the chance of risk of an intelligence failure.

...the changing security environment presents a need for updating the ASIO legislation. The current ASIO Act provisions do not cover the same range of national security threats, and do not reflect the modern concept of foreign intelligence as reflected in the [IS] Act. The ASIO Act provisions were drafted at a time when the main national security threats were state-sponsored threats, and therefore focused on defence and international affairs.<sup>20</sup>

3.16 The Department listed terrorism, transnational crime, weapons proliferation (including proliferation of nuclear, biological, chemical and conventional weapons and related technologies) and people smuggling as some examples of the types of modern national security threats that are increasingly not state sponsored.<sup>21</sup> An officer from the Department provided further examples of potential threats during questioning at a Budget Estimates 2011-12 hearing:

An example of that would be—and this is something that people do have in mind with these amendments—is major cyberattacks, for example. Nowadays much of our industry and much of our economic infrastructure, which is very, very connected to our national security, is owned by the private sector as well as the Australian government, the state government and the like and they can be targeted by individuals, not other countries, who could threaten our national economic wellbeing. A major organised crime syndicate which had been effective in attacking, say, our banks could cause a loss of confidence in the banking system and then do considerable damage to our economy. That would be an example of something major of that nature.

Another one, which is particularly important, is to do with the proliferation of nuclear biological, chemical and conventional weapons technology. In the old days, everyone would think: that would have to be controlled or initiated by a foreign power, which is the traditional side of it; however, there is a lot of money in it. There is a lot of money in these sorts of

---

19 *Second Supplementary Submission*, p. 5.

20 *Second Supplementary Submission*, p. 7.

21 *Submission 4*, p. 2; *Second Supplementary Submission*, p. 8.

activities, and so you could have individuals threatening our national economic wellbeing in that way.

Another final area, which is important, is the environment side such as illegal fishing operations or wiping out whole species of fish and the like. You could have a situation where you had individuals doing that and affecting our national wellbeing in that way.<sup>22</sup>

3.17 With respect to safeguards on the exercise of the foreign intelligence collection function, the Department reiterated that existing safeguards and requirements will continue to apply under the proposed amendments:

The safeguards under the Intelligence Services Act, including the requirement for a Ministerial authorisation, would continue to apply. This is because ASIO obtains foreign intelligence at the request of the other agencies. Therefore, before making a request of ASIO, those agencies would need to comply with their own legislation. In relation to the collection of foreign intelligence by ASIO, there would be an additional safeguard as the Attorney-General will be required to be satisfied that collecting particular intelligence is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic wellbeing. In making this decision, the Attorney-General receives advice from the Minister for Defence or the Minister for Foreign Affairs.<sup>23</sup>

### ***Role of the Inspector-General of Intelligence and Security***

3.18 The Department advised that the Inspector-General of Intelligence and Security (IGIS) 'regularly reviews ASIO's warrant documentation and in doing so has full access to all the warrant information, including the supporting evidence that was put forward to the Attorney-General'. The IGIS also 'looks at propriety which is not just about whether ASIO met the legislative requirements but encompasses all those other aspects that sit in and around it, including whether ASIO adhered to internal guidelines'.<sup>24</sup>

3.19 At the public hearing, the IGIS, Dr Vivienne Thom, informed the committee:

In general, I consider that it is not my role to comment on government policy, the operational requirements of the intelligence agencies or the legislative amendments which might be required to meet those policy requirements. But if I formed the view, based on my oversight activities, that any proposed amendments might compromise oversight arrangements or pose risks to propriety or human rights that may not be apparent from the face of the amendments, or if I believe that the organisation might not have

---

22 Committee Hansard, 25 May 2011, p. 87. See also *Second Supplementary Submission*, p. 8.

23 *Second Supplementary Submission*, p. 5; see also *Second Supplementary Submission*, pp 8-11.

24 *Second Supplementary Submission*, pp 10-11.

the adequate internal controls to implement new amendments then I would consider it appropriate that I should inform the committee of my views.<sup>25</sup>

3.20 Dr Thom addressed the Law Council's concerns regarding the threshold test:

While the new conditions recognise the broader nature of the contemporary threat environment, in my view the threshold of being in the interests of national security, Australia's foreign relations or national economic wellbeing are not insignificant or trivial. I would not paraphrase 'in the interests of' as 'somehow relevant to', as has been done in some of the submissions. When inspecting foreign intelligence collection warrant documentation, under the proposed regime we would be paying close attention to the documentation that addresses these criteria.<sup>26</sup>

3.21 At the hearing, some members of the committee raised concerns about the broad nature of the element of the new definition concerning 'Australia's economic well-being' and, in particular, the approach of the IGIS in her role or review of that element. An officer from the Department confirmed that this element is not defined, but the intention is that it would not concern any matters that are 'trivial' in nature. He emphasised that this phrase has been used in the IS Act for over 10 years.<sup>27</sup>

3.22 Dr Thom described her approach to review in regards to 'Australia's economic well-being' criterion:

[T]hat is ultimately a decision for the minister which I do not inquire into. What I would look at is the sort of case that ASIO have put forward, the information they have provided and, of course, the other agency that is involved, be it a foreign affairs agency or a defence agency. Is the information they have put forward to support the case balanced and thorough? Is the case that is put forward firmly based on the information they have?<sup>28</sup>

## **Immunity provisions in the IS Act and the Criminal Code**

3.23 Items 19 and 26 of Schedule 1 amend certain immunity provisions in the Criminal Code and the IS Act, respectively, for clarification to ensure the immunity provisions are not vulnerable to being inadvertently overridden by subsequent Commonwealth, state or territory laws, unless that law expressly states otherwise.

3.24 The Department's submission noted:

This provision provides immunity from civil and criminal activities for a limited range of circumstances directly related to the proper performance by the agencies of their functions. This limited immunity is necessary as

---

25 *Committee Hansard*, 16 June 2011, p. 8.

26 *Committee Hansard*, 16 June 2011, p. 8.

27 *Committee Hansard*, 16 June 2011, p. 9.

28 *Committee Hansard*, 16 June 2011, p. 10.

certain Australian laws, including State and Territory laws, could impose liability on the agencies. The proposed amendment will not prevent other laws from limiting this immunity. However, the amendment will ensure that any such limitation cannot be done inadvertently, and will require express consideration to be given to whether section 14 should be overridden.<sup>29</sup>

3.25 Subsection 476.5 of the Criminal Code provides immunity from civil and criminal liability for staff members and agents of ASIS, DSD and DIGO for computer-related activities carried out by the agencies in the proper performance of their functions, which might otherwise be prohibited by the unintended consequences of certain Australian laws. Item 19 of the Bill amends subsection 476.5 of the Criminal Code to ensure this immunity provision is not vulnerable to being inadvertently overridden by subsequent legislation, unless the law expressly states otherwise.<sup>30</sup>

3.26 The Department noted in its submission that this amendment mirrors the immunity provision in section 14 of the IS Act, described above, so it is desirable to maintain consistency between the two provisions.<sup>31</sup>

3.27 The Castan Centre for Human Rights Law considered that Items 19 and 26 are constitutionally unproblematic in relation to state and territory laws. However, it raised concerns with the application to Commonwealth legislation:

While there is scholarly support for the notion that the Commonwealth Parliament enjoys the power to require its own legislation to be amended, if at all, only by express words, there are contrary opinions. Some commentators take the view that a consequence of the Commonwealth Parliament's plenary legislative power (as stated in section 51 of the *Constitution*, and of course subject to the *Constitution* itself) is that the Parliament cannot deprive itself of the power of implied repeal by provisions such as those that items 19 and 26 would introduced into the law.<sup>32</sup>

3.28 However, the Department considered the Castan Centre's view of constitutional complications arising out of Items 19 and 26 to be 'overstated':

The normal rules of statutory construction provide that an earlier statutory provision is not repealed by a later provision unless an intention to that effect is implied (for example, the provisions are not capable of operating consistently). There is a general presumption that the legislature intends that both provisions should operate and that, to the extent they would otherwise overlap, one should be read as subject to the other.

---

29 *Submission 4*, p. 7.

30 EM, p. 7.

31 *Submission 4*, p. 7.

32 *Submission 2*, p. 5.



The proposed amendments would make it clear that the provisions are intended to prevail in the absence of an express contrary provision. This makes the legislature's intention clear as to the intended operation of the law. In the absence of clear indication by a later legislature that it intends to displace these express provisions and impliedly 'repeal' them, the proposed amendments to the immunity provisions may operate to affect the question of precedence between overlapping provisions in relevant cases.

The proposed amendments will not prevent other laws from limiting the immunity in these provisions as Parliament may choose to override these immunities in appropriate circumstances. The immunity provisions are not necessarily something that legislators would actively turn their mind to, and the risk of inadvertently overriding these provisions could therefore arise. However, the amendments will ensure that there would need to be a conscious decision to do so and it would need to be made express on the face of the legislation. This would ensure that any such limitation cannot be done inadvertently.<sup>33</sup>

## **ASIO computer access warrants**

3.29 Item 4 of the Bill amends the ASIO Act to clarify that computer access warrants authorise ongoing access to the computer during the life of the warrant. The EM notes that this amendment updates the language to ensure consistency throughout section 25A and to make clear the original legislative intent of the section.<sup>34</sup>

3.30 The submission of the Attorney-General's Department highlighted the existing safeguards concerning computer access warrants:

These amendments will not impact on the strong existing safeguards that ensure computer access warrants are only authorised in appropriate circumstances. A computer access warrant can only be issued by the Attorney-General in the prescribed circumstances set out in the provision – that is, the Attorney-General must be satisfied that there are reasonable grounds for believing that access by ASIO to data held in a particular computer will substantially assist the collection of intelligence...in respect of a matter that is important in relation to security. Additionally, the Attorney-General's Guidelines, issued under section 8A of the ASIO Act, require that 'any means used for obtaining information must be proportionate to the gravity of the threat posed and the probabilities of its occurrence', and 'using as little intrusion into individual privacy as is possible'. When a warrant is issued, the Director-General is required to report to the Attorney-General on the extent to which the warrant assisted ASIO in carrying out its functions.<sup>35</sup>

---

33 *Supplementary Submission*, p. 4.

34 EM, pp 4-5.

35 *Submission 4*, p. 3.

3.31 Dr Dan Svantesson raised concerns that the proposed amendment concerning computer access warrants may be inadequate as it limits access to the computer the warrant relates to, but not other possible data that may be associated with that computer through a 'cloud computing' arrangement.

A focus on such data risks becoming outdated in light of fast advancing cloud computing services. With cloud computing, person X's data will simply not be stored as such on person X's computer and a warrant to access data stored on that computer will be of limited value.

Imagine, for example, that a warrant is issued in relation to Mr X's computer (the "target computer"). Imagine further that, in accessing that computer it becomes clear that no substantial data is stored on the computer as Mr X uses a cloud computing structure for all his work. As the warrant is limited to Mr X's computer, it would seem that access would not be allowed to the cloud computing storage even if, for example, Mr X has stored his log-in details for that service on his computer.

Furthermore, under a cloud computing structure, it may not be possible to know in advance on what particular computer data is stored.<sup>36</sup>

3.32 In a supplementary submission, the Department addressed Dr Svantesson's concerns:

The Bill will amend paragraph 25A(4)(a) of the ASIO Act to replace 'stored in the target computer' with 'held in the target computer at any time while the warrant is in force'. This amendment is not intended to change the law, but rather to clarify the intent of the provision and ensure consistent language is used throughout the provision.

The scope of this amendment is to clarify that the intention was to authorise access to data held in the target computer at any time while the warrant is in force. This makes clear that the provision is intended to authorise access to data that is held in the target computer during the life of the warrant, and is not limited to data held at a particular point in time (such as when the warrant is first executed).<sup>37</sup>

3.33 The Department also expanded upon the definitions within the ASIO Act that deal with computer access warrant provisions:

Section 22 of the ASIO Act provides a number of definitions for the purpose of interpreting the computer access warrant provisions under section 25A of the ASIO Act. These definitions are technologically neutral and provide authoritative and useful definitions for ASIO in the exercise of its powers under section 25A. The definitions are wide enough to include various aspects of a computer and types of data. Under section 22 of the ASIO Act, computer means 'a computer, a computer system or part of a

---

36 *Submission 9*, p. 1.

37 *Supplementary Submission*, p. 4.

---

computer system' while the definition of data 'includes information, a computer program or part of a computer program'.<sup>38</sup>

## Committee view

3.34 The committee acknowledges that some submissions and witnesses raised important issues regarding certain proposed amendments in the Bill, particularly Items 3, 7 and 13 of Schedule 1 which will enable ASIO to collect a broader range of foreign intelligence than is currently possible. However, the committee believes that the proposed amendments are necessary to ensure that ASIO is able to respond to modern national security threats which encompass both state and non-state actors. Further, the committee agrees that the Bill's proposed measures will provide for a consistent approach across relevant intelligence agencies in Australia.

3.35 The proposed amendments to the ASIO Act relating to foreign intelligence will allow ASIO to fulfil its intended role of complementing the foreign intelligence function of other intelligence agencies. The committee has confidence in the integrity and conduct of ASIO in relation to any collection of foreign intelligence under the proposed amendments, and is of the view that the expansion of ASIO's powers in this regard are necessary to enable it to continue to act lawfully in dealing with the changing nature of potential security threats to Australia.

3.36 In that context, the committee notes assurances by the Department as follows:

In exercising their powers, agencies are necessarily focused on performing their statutory functions and they do not have the resources or legislative mandate to engage in unwarranted or lower level activity. Agencies would only look into matters of high importance to the national interest...[and] relevant safeguards...ensure the propriety and legality of ASIO's exercise of their functions and powers, including the monitoring, inspection and inquiry powers of the IGIS.<sup>39</sup>

3.37 The committee agrees that the proposed amendments will improve the practical operation of some key provisions in relevant legislation, while maintaining sufficient safeguards where appropriate. In addition, the committee has confidence that the oversight by the IGIS to review the legality and propriety of activities of agencies within the Australian intelligence community, including monitoring, inspection and inquiry powers, is a sufficient and appropriate safeguard.

3.38 The measures in the Bill should be considered as key priorities in the current security environment, and the committee believes the Bill should be passed in a timely manner to ensure Australia's security and intelligence agencies have the ability to respond to the changing nature of threats to national security as soon as possible.

---

38 *Supplementary Submission*, p. 5.

39 *Second Supplementary Submission*, p. 8.

3.39 As a final point, however, the committee expresses its disappointment with the overall quality of the Explanatory Memorandum (EM) produced to accompany the Bill. The lack of detail in the EM, particularly in relation to the proposed foreign intelligence amendments, did not assist the committee in undertaking its consideration of the legislation. The EM does not provide a detailed explanation of the need for the provisions and how the expansion of ASIO's powers will assist it and other foreign intelligence agencies to perform their functions, nor does it mention the safeguards in place that will ensure appropriate use of the enhanced powers.

3.40 Given the opposition to the foreign intelligence provisions by a number of submitters and witnesses, this is a significant omission, and it would have been of great assistance if a more comprehensive explanation had been provided in the EM. The information subsequently provided by the Department to the committee (particularly in its second supplementary submission) was extremely helpful and, in the committee's view, should have been included in the EM in the first place. The committee recommends that this oversight be corrected immediately by way of revision and reissue of the EM to include all additional information provided to the committee during the course of the inquiry which relates to the proposed foreign intelligence amendments contained in the Bill.

### **Recommendation 1**

**3.41 The committee recommends that the Attorney-General's Department revise and reissue the Explanatory Memorandum to the Bill as a matter of urgency to specifically include all additional information contained in the Department's submissions to this inquiry which relate to the proposed foreign intelligence amendments in Items 3, 7 and 13 of Schedule 1 of the Bill, including:**

- **detailed justification and explanation of why the amendments are considered necessary;**
- **specific examples of how the expansion of the definition of 'foreign intelligence' will assist ASIO and other foreign intelligence agencies to perform their functions; and**
- **an explanation of the safeguards in place to ensure appropriate use of the foreign intelligence collection function.**

### **Recommendation 2**

**3.42 Subject to Recommendation 1, the committee recommends that the Senate pass the Bill.**

**Senator Trish Crossin  
Chair**