

CHAPTER 2

OVERVIEW OF THE BILL

Background

2.1 The Attorney-General, in his second reading speech, advised that the proposed amendments in the Bill are part of the government's ongoing review of national security legislation and 'have been identified through practical experience' as measures to improve the operation of the key provisions of the legislation to be amended.¹

2.2 In announcing these proposed amendments, the Attorney-General also noted that Australia's intelligence and security agencies continue to be subject to a range of oversight and accountability measures, including the Parliamentary Joint Committee on Intelligence and Security and the Inspector-General of Intelligence and Security.²

Summary of provisions

2.3 The Bill amends the *Australian Security Intelligence Organisation Act 1979*, (ASIO Act) the *Criminal Code Act 1995* (Criminal Code) and the *Intelligence Services Act 2001* (IS Act).

Amendments to the ASIO Act

Definitions

2.4 Items 1 and 2 of Schedule 1 insert a definition for 'Defence Minister' and 'Foreign Affairs Minister' into section 4 of the ASIO Act. The Explanatory Memorandum (EM) notes that the definitions to be inserted are consistent with the way the Defence and Foreign Affairs ministers are defined in other legislation.³

2.5 To ensure that the collection of foreign intelligence under the ASIO Act encompasses the same range of intelligence about state and non-state threats as provided for in the IS Act and the *Telecommunications (Interception and Access) Act 1979* (TIA Act), Item 3 of Schedule 1 repeals the current definition of 'foreign intelligence' and substitutes an amended definition consistent with those Acts.⁴ This amendment changes the definition of 'foreign intelligence' from 'intelligence relating to the capabilities, intentions or activities of a foreign power' where 'foreign power' means 'a foreign government; an entity that is directed or controlled by a foreign

1 The Hon Robert McClelland MP, Attorney-General, *House Hansard*, 23 March 2011, p. 2862.

2 The Hon Robert McClelland MP, Attorney-General, *House Hansard*, 23 March 2011, p. 2862.

3 EM, p. 4.

4 EM, p. 4.

government or governments; or a foreign political organisation' to 'intelligence about the capabilities, intentions or activities of people or organisations outside Australia.'

2.6 The Minister noted in his second reading speech that this amendment:

...ensures a consistent approach to the collection of foreign intelligence and reflect[s] that the modern national security context encompasses threats from both state and non-state actors.⁵

Computer access warrants

2.7 Item 4 of Schedule 1 amends paragraph 25A(4)(a) of the ASIO Act dealing with the 'things' that may be authorised in a computer access warrant. It clarifies the intent of the existing provision to ensure that such a warrant authorises access to data held in the target computer at any time while the warrant is in force, and is not limited to data held at a particular point in time. This proposed amendment will also ensure consistency with the language used throughout section 25.⁶

2.8 The EM notes that this amendment is not intended to change the operation of the provision.⁷

Issue of warrants for foreign intelligence collection

2.9 Items 5 and 6 make consequential amendments to paragraph 27A(1)(a); and Items 8 to 10 make consequential amendments to subsections 27A(1) and (3) regarding the issuing of warrants, to provide clarification that references to the 'Minister' mean the Minister responsible for issuing warrants under section 27A.

2.10 Item 7 repeals and replaces paragraph 27A(1)(b) to amend the conditions for the issue of foreign intelligence warrants, bringing the ASIO Act into alignment with the IS Act and TIA Act. The current conditions for the issue of such a warrant is that the issuing Minister must be satisfied that, on the basis of advice received, the collection of foreign intelligence relating to that matter is important in relation to the defence of the Commonwealth or to the conduct of the Commonwealth's international affairs. The proposed amendment broadens the conditions, so that the matter can be in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being.

Authorising foreign intelligence collection

2.11 Item 13 repeals and replaces paragraph 27B(b) to amend and broaden the conditions for authorising foreign intelligence collection. Similar to Item 7, this

5 The Hon Robert McClelland MP, Attorney-General, *House Hansard*, 23 March 2011, p. 2861.

6 EM, p. 5.

7 EM, p. 5.

amendment will align the ASIO Act with the relevant provisions in the IS Act and TIA Act.⁸

2.12 Currently under section 27B of the ASIO Act, the Attorney-General must be satisfied, on the basis of advice received from the relevant Minister, that the collection of foreign intelligence relating to that matter is important in relation to the defence of the Commonwealth or to the conduct of the Commonwealth's international affairs.

2.13 Under the amended paragraph 27B(b), the authorising Minister will have the ability to authorise the collection of foreign intelligence if satisfied, on the basis of relevant advice, that the collection relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being.

2.14 Items 11 and 12, and Items 14 and 15 make consequential amendments to paragraph 27B(a) and section 27B respectively, to ensure that references to the Minister are references to the Minister responsible for granting authorisations.

Communication of information relating to employment decisions

2.15 Item 18 amends section 36 in Part IV of the ASIO Act, relating to security assessments, to exclude the communication by ASIO of information relating to the engagement, or proposed engagement, of a person by ASIO or another intelligence or security agency within the Australian intelligence community (AIC).⁹

2.16 The EM states that:

The amendment will ensure that ASIO can share information about employment decisions with other members of the AIC. This might include information in response to inquiries about a person's employment or proposed employment with ASIO or another AIC agency, information about security clearances and other related information. Other AIC agencies are already able to share this information and are not subject to the same administrative requirements that apply to ASIO (which includes notification and review rights). Therefore, this amendment will put ASIO on the same footing as other AIC agencies when it comes to sharing information relating to employment within the AIC. This is a very limited category of information, and the amendment will only impact on a small group of persons. Employment decisions within the AIC need to be made carefully, and necessarily the processes take quite some time compared to other Government employment processes in order to ensure suitability of applicants and minimise risk of compromising national security.¹⁰

8 EM, p. 6.

9 EM, p. 7.

10 EM, p. 7.

2.17 Item 16 inserts a definition of 'agency head' into subsection 35(1) of the ASIO Act for the purpose of the proposed amendment under Item 18 and includes the head of each of the six AIC agencies.

2.18 Similarly, Item 17 inserts a definition of 'staff member' into subsection 35(1) of the ASIO Act as a consequence of the proposed amendment under Item 18. The definition is broad and covers a range of employment arrangements for staff of the six AIC agencies. The EM explains:

These agencies operate under differing legislative provisions, and therefore have differing employment provisions, so this definition needs to cover all such employment arrangements.¹¹

Amendment to the Criminal Code

Immunity from civil and criminal liability relating to computer offences

2.19 Item 19 amends subsection 476.5(2A) of the Criminal Code. This subsection provides immunity from civil and criminal liability for staff members or agents of the Australian Secret Intelligence Service (ASIS), Defence Imagery and Geospatial Organisation (DIGO) or Defence Signals Directorate (DSD) for computer-related activities carried out by the agencies in the proper performance of their functions, which might otherwise be prohibited by the unintended consequence of certain Australian laws.

2.20 The proposed amendment inserts a clause into existing subsection 476.5(2A) to ensure that the immunity provision is not inadvertently overridden by subsequent Commonwealth, state or territory legislation, unless that law expressly states otherwise.¹²

2.21 The EM notes that this amendment is complementary to the amendment made by Item 26.¹³

Amendments to the IS Act

Amendments to make express the status of certain instruments

2.22 Proposed amendments under Items 20, 22, 27 and 28 of Schedule 1 'make express' the status of certain instruments made under the IS Act.¹⁴

2.23 The EM notes that these amendments are consistent with the recommendations from the *2008 Review into the Legislative Instruments Act 2003*

11 EM, p. 6.

12 EM, p. 7.

13 EM, p. 7.

14 EM, pp 7-8 and 9-10.

where it indicated a preference for exemptions to be included in the primary Act rather than the *Legislative Instruments Regulations 2004* (Legislative Instruments Regulations).¹⁵ In that context, the EM explains the purpose of the proposed amendments:

This makes laws clearer and means that it is only necessary to consult the primary Act to ascertain whether an instrument is a legislative instrument. Therefore th[ese] item[s] move the exemption from the Regulations into the *Intelligence Services Act 2001*.¹⁶

2.24 The EM clarifies that the proposed amendments under Items 20, 22, 27 and 28 do not change the law, as any instruments made under the relevant sections to be amended are already exempt from the *Legislative Instruments Act 2003* (Legislative Instruments Act), and this is stated in the Legislative Instruments Regulations.¹⁷

Ministerial directions

2.25 Items 20 and 22 will amend subsection 6(3) and section 8 of the IS Act relating to ministerial directions. The amendments provide that a direction given by the responsible Minister under paragraph 6(1)(e) and section 8 are not legislative instruments.¹⁸

Rules to protect privacy of Australians

2.26 Item 27 inserts new subsection 15(7) into the IS Act to clarify the status of instruments made under section 15 of that Act which deals with rules to protect the privacy of Australians. The amendment provides that rules made under this section are not legislative instruments.

Guidelines related to the use of weapons and self-defence techniques

2.27 Item 28 will insert a new subclause 8 at the end of clause 1 of Schedule 2 of the IS Act to clarify the status of instruments made under subclause 1(6) of Schedule 2 of that Act dealing with the guidelines issued by the Director-General on matters related to the use of weapons and self-defence. This amendment provides that guidelines issued under subclause (6) are not legislative instruments.

Functions of DIGO

2.28 Section 6B of the IS Act relating to the functions of DIGO is amended by Item 21 of Schedule 1. This amendment inserts proposed new paragraph 6B(g) to expressly allow DIGO to provide assistance to the Australian Defence Force in

15 EM, pp 8-10.

16 EM, pp 8-10.

17 EM, pp 8-10.

18 EM, p. 8.

support of military operations and to cooperate with the Defence Force on intelligence matters .

2.29 The EM notes:

This is not an extension of the functions of DIGO but a clarification of them. The function is consistent with a similar function of the Defence Signals Directorate.¹⁹

Ministerial authorisation for producing intelligence about Australian persons

2.30 Item 23 of Schedule 1 inserts new subparagraph 9(1A)(a)(iva) into the IS Act to provide an additional ground for obtaining a Ministerial Authorisation under that section.

2.31 The IS Act requires a Ministerial Authorisation for ASIS, DSD or DIGO to undertake activities for the purpose of producing intelligence on an Australian person and requires the Minister to be satisfied that the person is, or is likely to be, involved in one or more of the activities listed in paragraph 9(1A)(a).²⁰

2.32 This item will amend the grounds for such an authorisation under paragraph 9(1A)(a), to include as a ground that the Australian person is, or is likely to be, involved in activities related to a contravention, or an alleged contravention, of a 'UN sanction enforcement law'.²¹

2.33 Item 24 inserts a definition of 'UN sanction enforcement law' in subsection 9(1B) of the IS Act for the purpose of the amendment made by Item 23, and provides that the term has the same meaning as in the *Charter of the United Nations Act 1945*.

Immunity from civil and criminal liability for certain acts

2.34 Item 26 will amend section 14 of the IS Act in a similar way to the proposed amendment under Item 19 to the Criminal Code (discussed in paragraphs 2.19-2.21 above).

2.35 Section 14 provides immunity from civil and criminal liability for staff members and agents of an agency (ASIS, IGO or DSD) for 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.

19 EM, p. 8.

20 EM, p. 9. These activities include, for example, activities that present a significant risk to a person's safety; acting for, or on behalf of, a foreign power; or committing a serious crime by using or transferring intellectual property.

21 EM, p. 9.

2.36 The proposed amendments will insert two new subsections into section 14 to ensure the immunity provision is not vulnerable to being overridden by other Commonwealth, state or territory laws, unless that law expressly states otherwise.²²

22 EM, p. 9.