National Security Legislation Amendment Act (No. 1) 2014

No. 108, 2014

An Act to amend the law relating to national security and intelligence services, and for related purposes

Note: An electronic version of this Act is available in ComLaw (http://www.comlaw.gov.au/)

Contents

1 Short title 1
2 Commencement 2
3 Schedule(s) 2

Schedule 1—ASIO employment etc. 4

Part 1—Main amendments 4

Australian Security Intelligence Organisation Act 1979 4

Part 2—Other amendments 12

Administrative Appeals Tribunal Act 1975 12

Australian Postal Corporation Act 1989 12

Crimes Act 1914 13

Criminal Code Act 1995 13

Inspector-General of Intelligence and Security Act 1986 14

Public Interest Disclosure Act 2013 15

Surveillance Devices Act 2004 16

Taxation Administration Act 1953 16

Telecommunications (Interception and Access) Act 1979 17

Part 3—Transitional and application provisions 21

Schedule 2—Powers of the Organisation 25

Part 1—Amendments 25

Australian Security Intelligence Organisation Act 1979 25

Part 2—Consequential amendments 61

Telecommunications (Interception and Access) Act 1979 61

Part 3—Application, transitional and savings provisions 62

Schedule 3—Protection for special intelligence operations 63

Australian Security Intelligence Organisation Act 1979 63

Schedule 4—ASIO co-operation and information sharing 76

Australian Security Intelligence Organisation Act 1979 76

Schedule 5—Activities and functions of Intelligence Services Act 2001 agencies 77
Intelligence Services Act 2001 77
Schedule 6—Protection of information 85
Part 1—Main amendments 85
Australian Security Intelligence Organisation Act 1979 85
Intelligence Services Act 2001 91
Part 2—Consequential amendments 115
Australian Crime Commission Act 2002 115
Crimes Act 1914 115
Privacy Act 1988 115
Schedule 7—Renaming of Defence agencies 116
Part 1—Main amendments 116
Intelligence Services Act 2001 116
Part 2—Consequential amendments 122
Anti-Money Laundering and Counter-Terrorism Financing Act 2006 122
Archives Act 1983 123
Australian Human Rights Commission Act 1986 123
Australian Security Intelligence Organisation Act 1979 124
Crimes Act 1914 125
Crimes (Overseas) Act 1964 126
Criminal Code Act 1995 126
Freedom of Information Act 1982 127
Independent National Security Legislation Monitor Act 2010 129
Inspector-General of Intelligence and Security Act 1986 129
Privacy Act 1988 131
Public Interest Disclosure Act 2013 132
Part 3—Transitional provisions 133

National Security Legislation Amendment Act (No. 1) 2014

No. 108, 2014

An Act to amend the law relating to national security and intelligence services, and for related purposes

[*Assented to 2 October 2014*]

The Parliament of Australia enacts:

1 Short title

This Act may be cited as the *National Security Legislation Amendment Act (No. 1) 2014*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provision(s)	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	2 October 2014
2. Schedules 1 to 6	The 28th day after this Act receives the Royal Assent.	30 October 2014
3. Schedule 7, items 1 to 110	The day after this Act receives the Royal Assent.	3 October 2014
4. Schedule 7, items 111 to 114	The day after this Act receives the Royal Assent. However, if item 1 of Schedule 1 to the *Independent National Security Legislation Monitor Repeal Act 2014* commences at or before that time, the provision(s) do not commence at all.	3 October 2014
5. Schedule 7, items 115 to 145	The day after this Act receives the Royal Assent.	3 October 2014

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedule(s)

Each Act that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule

concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—ASIO employment etc.

Part 1—Main amendments

Australian Security Intelligence Organisation Act 1979

1 Section 4

Insert:

> ***ASIO affiliate*** means a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement, and includes a person engaged under section 85 and a person performing services under an agreement under section 87, but does not include the Director-General or an ASIO employee.
>
> ***ASIO employee*** means a person employed under section 84 or 90.

2 Section 4 (definition of *Deputy Director-General*)

Omit "an officer of the Organisation who holds office", substitute "a person who holds, or is acting in, a position known".

3 Section 4

Insert:

> ***senior position-holder*** means an ASIO employee, or an ASIO affiliate, who holds, or is acting in, a position in the Organisation that is:
>
> (a) equivalent to or higher than a position occupied by an SES employee; or
>
> (b) known as Coordinator.

4 Paragraph 8A(1)(b)

Omit "sections 85 and 86", substitute "sections 84, 85, 86 and 87".

5 Section 16

Repeal the section, substitute:

16 Delegation

(1) The Director-General may, by signed writing, delegate to a person any of the Director-General's powers, functions or duties under or for the purposes of this Act that relate to:
  (a) the management of ASIO employees or ASIO affiliates; or
  (b) the financial management of the Organisation.

Note: For further provisions relating to delegations, see sections 34AB and 34A of the *Acts Interpretation Act 1901*.

(2) In exercising powers, performing functions or discharging duties under a delegation, the delegate must comply with any written direction given by the Director-General to the delegate.

6 Subsection 18(2)

Repeal the subsection (not including the penalty), substitute:

Offence for unauthorised communication of information or matter

(2) A person commits an offence if:
  (a) the person makes a communication of any information or matter; and
  (b) the information or matter has come to the knowledge or into the possession of the person by reason of:
    (i) his or her being, or having been, an ASIO employee; or
    (ii) his or her being, or having been, an ASIO affiliate; or
    (iii) his or her having entered into a contract, agreement or arrangement with ASIO (otherwise than as an ASIO affiliate); and
  (c) the information or matter:
    (i) was acquired or prepared by or on behalf of the Organisation in connection with its functions; or
    (ii) relates to the performance by the Organisation of its functions; and
  (d) the communication was not made to the Director-General, an ASIO employee or an ASIO affiliate:
    (i) by an ASIO employee, in the course of the ASIO employee's duties; or
    (ii) by an ASIO affiliate, in accordance with the contract, agreement or other arrangement under which the ASIO

affiliate is performing functions or services for the Organisation; or

(iii) by a person who has entered into a contract, agreement or arrangement with ASIO (otherwise than as an ASIO affiliate), in accordance with the contract, agreement or arrangement; and

(e) the communication was not made by a person acting within the limits of authority conferred on the person by the Director-General; and

(f) the communication was not made with the approval of the Director-General or of a person having the authority of the Director-General to give such an approval.

7 Subsection 19A(3)

Omit "officers and employees, and other resources, of the Organisation", substitute "ASIO employees and ASIO affiliates, and other resources of the Organisation,".

8 Subsection 23(1)

Omit "an authorised officer or employee", substitute "the Director-General or an authorised person".

9 Subsection 23(6)

Repeal the subsection, substitute:

(6) The Director-General, or a person appointed under subsection (6A), may authorise, in writing, a person, or a class of persons, for the purposes of this section.

(6A) The Director-General may, in writing, appoint a senior position-holder, or a class of senior position-holders, for the purposes of subsection (6).

10 Subsection 23(7) (definition of *authorised officer or employee*)

Repeal the definition.

11 Subsection 23(7)

Insert:

authorised person means a person who is authorised under subsection (6) for the purposes of this section.

12 Subsection 23(7) (definition of *senior officer of the Organisation*)

Repeal the definition.

13 Subsection 25A(4) (note)

Omit "an ASIO officer", substitute "a person".

14 Subsection 25A(4) (note)

Omit "the ASIO officer", substitute "the person".

15 Subsections 27(1) and 27AA(1)

Omit "an officer, employee or agent of the Organisation" (wherever occurring), substitute "the Director-General, an ASIO employee or an ASIO affiliate".

16 Paragraph 34ZC(2)(c)

Repeal the paragraph, substitute:

(c) an ASIO employee or an ASIO affiliate;

17 Subparagraph 34ZE(7)(c)(iii)

Repeal the subparagraph, substitute:

(iii) an ASIO employee or an ASIO affiliate;

18 Part V (heading)

Repeal the heading, substitute:

Part V—ASIO employees etc.

19 Sections 84 to 89

Repeal the sections, substitute:

84 Employees of the Organisation

Employees

(1) The Director-General may, on behalf of the Commonwealth, employ such persons as he or she considers necessary for the performance of the Organisation's functions and the exercise of the Organisation's powers.

(2) The Director-General may from time to time determine in writing the terms and conditions of employment applying to persons employed under subsection (1).

(3) The Director-General, on behalf of the Commonwealth, has all the rights, duties and powers of an employer in respect of persons employed under subsection (1).

(4) Without limiting subsection (3), the Director-General has, in respect of persons employed under subsection (1), the rights, duties and powers that are prescribed by regulation.

Termination of employment

(5) The Director-General may, at any time, by written notice, terminate the employment of a person employed under subsection (1).

Note: The *Fair Work Act 2009* has rules and entitlements that apply to termination of employment.

85 Consultants and contractors

(1) The Director-General may engage persons as consultants or contractors to the Organisation.

(2) An engagement under subsection (1) is to be made:
(a) on behalf of the Commonwealth; and
(b) by written agreement.

86 Secondment of ASIO employees

Secondment

(1) The Director-General may, in writing, arrange for an ASIO employee to be seconded for a specified period to a body or organisation whether within or outside Australia.

Termination of secondment

(2) The Director-General may at any time, by notice given to the body or organisation to which an ASIO employee is seconded under subsection (1), terminate the secondment.

87 Secondment of persons to the Organisation

(1) The Director-General may, by written agreement with a body or organisation (whether within or outside Australia), arrange for a person who is an officer, employee or other member of staff of the body or organisation to be made available to the Organisation to perform services in connection with the performance or the exercise of any of the Organisation's functions or powers.

(2) The terms and conditions (including remuneration and allowances) applicable to a person performing services under an agreement are those specified in the agreement.

88 Applicability of principles of the *Public Service Act 1999*

Although ASIO employees are not employed under the *Public Service Act 1999*, the Director-General must adopt the principles of that Act in relation to ASIO employees to the extent to which the Director-General considers they are consistent with the effective performance of the functions of the Organisation.

89 Voluntary moves to APS

(1) Section 26 of the *Public Service Act 1999* applies in relation to an ASIO employee as if the ASIO employee were an APS employee and the Organisation were an APS Agency.

(2) An ASIO employee who moves to an APS Agency under that section is entitled to have his or her employment, as an ASIO employee, treated as if it were:

(a) employment as an APS employee; and

(b) at a corresponding classification, as agreed between the Director-General and the Australian Public Service Commissioner.

20 Section 90 (heading)

Repeal the heading, substitute:

90 Regulations relating to employment of persons

21 Subsection 90(1)

Omit "officers otherwise than under agreements in writing and may, in respect of officers", substitute "persons otherwise than under section 84 and may, in respect of persons".

22 Subsection 90(2)

Repeal the subsection.

23 Subsection 90(2A)

Omit "persons who are or have been officers or temporary or casual employees", substitute "persons who are ASIO employees, ASIO affiliates, former ASIO employees or former ASIO affiliates".

24 Subsection 90(3)

Omit "notwithstanding sections 84, 85 and 86", substitute "despite section 84".

25 Subsection 90(4)

Repeal the subsection.

26 Section 91

Omit "officers and employees of the Organisation", substitute "ASIO employees and ASIO affiliates".

27 Section 92 (heading)

Repeal the heading, substitute:

92 Publication of identity of ASIO employee or ASIO affiliate

28 Subsection 92(1)

Omit all the words after "residing at", substitute:

a particular address, is:

(a) an ASIO employee or ASIO affiliate, or is in any way connected with an ASIO employee or ASIO affiliate; or

(b) subject to subsection (1B), is a former ASIO employee or former ASIO affiliate or is in any way connected with a former ASIO employee or former ASIO affiliate.

29 Subsection 92(1A)

Omit all the words after "residing at", substitute:

a particular address, is:

(a) an ASIO employee or ASIO affiliate, or is in any way connected with an ASIO employee or ASIO affiliate; or

(b) subject to subsection (1B), is a former ASIO employee or former ASIO affiliate, or is in any way connected with a former ASIO employee or former ASIO affiliate.

30 Subsection 92(1B)

Omit "former officer, employee or agent of the Organisation" (wherever occurring), substitute "former ASIO employee or former ASIO affiliate".

Part 2—Other amendments

Administrative Appeals Tribunal Act 1975

31 Subsection 3(1)

Insert:

ASIO affiliate has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

ASIO employee has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

32 Subsections 19(3B), 21AA(3) and 21AB(3)

Omit "an officer, employee or agent of the Australian Security Intelligence Organisation", substitute "an ASIO employee or ASIO affiliate".

33 Subsection 39A(15)

Repeal the subsection, substitute:

(15) If a person invited or summoned to give evidence under subsection (14) is:

(a) an ASIO employee or ASIO affiliate; or

(b) an officer or employee of the Commonwealth agency to which the assessment was given;

subsection (8) applies as if any evidence to be given by the person were evidence proposed to be adduced by or on behalf of the Director-General of Security or that agency, as the case may be.

Australian Postal Corporation Act 1989

34 Subsection 90F(1)

Omit "an officer or employee of ASIO", substitute "a person".

35 Paragraph 90F(2)(b)

Omit "an officer or employee of ASIO", substitute "a person".

36 Paragraph 90LD(2)(a)

Repeal the paragraph, substitute:

(a) the person is an ASIO employee (within the meaning of the ASIO Act) or an ASIO affiliate (within the meaning of that Act) and the information or document is or may be relevant to security (within the meaning of that Act); or

Crimes Act 1914

37 Paragraph 15LH(3) (paragraph (f) of the definition of *senior officer*)

Omit "senior officer of the Australian Security Intelligence Organisation as defined in section 24 of the *Australian Security Intelligence Organisation Act 1979*, or a person occupying an equivalent or higher position in the Australian Security Intelligence Organisation", substitute "senior position-holder within the meaning of the *Australian Security Intelligence Organisation Act 1979*".

Criminal Code Act 1995

38 Subsection 100.1(1) of the *Criminal Code*

Insert:

ASIO affiliate has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

ASIO employee has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

39 Subparagraph 105.39(2)(b)(vi) of the *Criminal Code*

Omit "officer or employee of the Australian Security Intelligence Organisation", substitute "ASIO employee or an ASIO affiliate".

40 Subsections 105.42(2) and (3) of the *Criminal Code*

Omit "officer or employee of the Australian Security Intelligence Organisation", substitute "ASIO employee or an ASIO affiliate".

41 Subparagraph 105.43(11)(c)(iv) of the *Criminal Code*

Omit "officer or employee of the Australian Security Intelligence Organisation", substitute "ASIO employee or an ASIO affiliate".

Inspector-General of Intelligence and Security Act 1986

42 Subsection 3(1)

Insert:

ASIO affiliate has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

ASIO employee has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

43 Paragraph 8(1)(b)

Omit "employees of ASIO", substitute "ASIO employees and ASIO affiliates".

44 Paragraph 8(7)(a)

Omit "Director-General of Security or ASIO employees", substitute "Director-General of Security, ASIO employees or ASIO affiliates".

45 After subsection 8(7)

Insert:

(8) The functions of the Inspector-General include inquiring into a matter to which a complaint to the Inspector-General made by an ASIO affiliate relates to the extent that the matter is related to:

(a) the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for ASIO; or

(b) the performance of functions or services by the ASIO affiliate under the contract, agreement or other arrangement.

(8A) However, the Inspector-General may decide not to inquire into a matter referred to in subsection (8) if the Inspector-General is satisfied that the ASIO affiliate can have the matter reviewed by a body constituted by, or including, persons other than the Director-General of Security, ASIO employees or ASIO affiliates.

46 Paragraph 11(5)(a)

Omit "employees of that agency", substitute "ASIO employees or ASIS employees (as the case may be)".

47 At the end of paragraph 11(5)(a)

Add "or".

48 At the end of section 11

Add:

(6) The Inspector-General may decide not to inquire into the matters to which a complaint of the kind referred to in subsection 8(8) relates in respect of action taken by ASIO if the Inspector-General is satisfied that:

(a) the procedures of ASIO relating to redress of grievances of ASIO affiliates are adequate and effective; or

(b) the complainant has not pursued those procedures as far as practicable; or

(c) the matters to which the complaint relates are not of sufficient seriousness or sensitivity to justify an inquiry into those matters.

Public Interest Disclosure Act 2013

49 Subparagraph 41(1)(f)(i)

Omit "or the Australian Security Intelligence Organisation".

50 After paragraph 41(1)(f)

Insert:

(fa) information:

(i) that identifies a person as an ASIO employee (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), an ASIO affiliate (within the meaning of that Act), a former ASIO employee, or a former ASIO affiliate, other than a person referred to in subsection (4); or

(ii) from which the identity of such a person could reasonably be inferred; or

(iii) that could reasonably lead to the identity of such a person being established;

51 Subsection 41(3)

Repeal the subsection, substitute:

(3) Paragraph (1)(f) does not apply to the Director-General of ASIS, or a person who has been determined by the Director-General of ASIS under this subsection.

(4) Paragraph (1)(fa) does not apply to the Director-General of Security, or a person who has been determined by the Director-General of Security under this subsection.

52 Section 66 (table item 7)

Omit "agency to which the agent or member of the staff referred to in that paragraph belongs", substitute "Australian Secret Intelligence Service".

53 Section 66 (after table item 7)

Insert:

7A	Paragraph 41(1)(fa)	The Australian Security Intelligence Organisation.

Surveillance Devices Act 2004

54 Subparagraph 45(4)(e)(i)

Omit "officer or employee of the Australian Security Intelligence Organisation", substitute "ASIO employee (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) or an ASIO affiliate (within the meaning of that Act)".

Taxation Administration Act 1953

55 Paragraph 355-70(2)(b) in Schedule 1

Omit "any other individual employed under paragraph 84(1)(a) or (b) of that Act", substitute "an ASIO employee (within the meaning of that Act) or an ASIO affiliate (within the meaning of that Act)".

56 Paragraphs 355-185(1)(c) and (2)(c) in Schedule 1

Omit "officers or employees of ASIO", substitute "ASIO employees (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) or ASIO affiliates (within the meaning of that Act)".

Telecommunications (Interception and Access) Act 1979

57 Subsection 5(1)

Insert:

ASIO affiliate has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

ASIO employee has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

58 Subsection 5(1) (definition of *Deputy Director-General of Security*)

Omit "an officer of the Organisation who holds office", substitute "a person who holds, or is acting in, a position known".

59 Section 5AD

Omit "senior officer of the Organisation (within the meaning of section 24", substitute "senior position-holder (within the meaning".

60 Paragraph 7(2)(ac)

Omit "officer of the Organisation", substitute "ASIO employee".

61 After paragraph 7(2)(ac)

Insert:

(ad) the interception of a communication where the interception results from, or is incidental to, action taken by an ASIO affiliate, in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation, for the purpose of:

(i) discovering whether a listening device is being used at, or in relation to, a particular place; or

(ii) determining the location of a listening device; or

62 Section 12

Omit "an officer of the Organisation", substitute "an ASIO employee or ASIO affiliate".

63 Section 12

Omit "officers and employees of the Organisation and other persons", substitute "any persons".

64 Subsection 18(4)

Omit all the words after "respect", substitute:

to anything done by an ASIO employee or an ASIO affiliate:

(a) in connection with the execution of a warrant issued under this Part; or

(b) in connection with:

(i) the communication by a person to another person of; or

(ii) the making use of; or

(iii) the making of a record of; or

(iv) the custody of a record of; or

(v) the giving in evidence of;

information obtained by the execution of such a warrant.

65 Paragraph 55(3)(c)

Repeal the paragraph, substitute:

(c) ASIO employees (or classes of ASIO employees);

66 Subsection 55(8)

Omit "officer or employee of the Organisation", substitute "ASIO employee".

67 Subsection 64(2)

Omit "officer or employee of the Organisation", substitute "ASIO employee or ASIO affiliate".

68 Paragraph 108(2)(g)

Omit "an officer of the Organisation", substitute "an ASIO employee".

69 After paragraph 108(2)(g)

Insert:

(ga) accessing a stored communication if the access results from, or is incidental to, action taken by an ASIO affiliate, in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation, for the purpose of:

(i) discovering whether a listening device is being used at, or in relation to, a particular place; or

(ii) determining the location of a listening device; or

70 Subsections 136(2) and (3)

Omit "officer or employee of the Organisation", substitute "ASIO employee or ASIO affiliate".

71 Subsection 136(3)

Omit "such officer or employee", substitute "ASIO employee or ASIO affiliate".

72 Subsection 136(4)

Omit "officer or employee of the Organisation", substitute "ASIO employee or ASIO affiliate".

73 Subsection 174(2)

Omit "an officer or employee of the Organisation", substitute "any other ASIO employee or ASIO affiliate".

74 Section 175

Omit "officer or employee of the Organisation" (wherever occurring), substitute "ASIO employee or ASIO affiliate".

75 Paragraph 176(2)(c)

Omit "officer or employee of the Organisation", substitute "ASIO employee or ASIO affiliate".

76 Subsections 184(1) and (2)

Omit "officer or employee of the Organisation", substitute "ASIO employee or ASIO affiliate".

77 Paragraphs 185B(1)(a) and (b)

Omit "officer or employee of the Organisation", substitute "ASIO employee or ASIO affiliate".

Part 3—Transitional and application provisions

78 Transitional—delegations

(1) This item applies to a delegation if the delegation was in force under section 16 of the *Australian Security Intelligence Organisation Act 1979* immediately before the commencement of this Schedule.

(2) The delegation has effect, after that commencement, as if the delegation had been made under section 16 of that Act as amended by this Schedule.

79 Transitional—requesting information or documents from operators of aircraft or vessels

(1) If, immediately before the commencement of this Schedule, a person was an authorised officer or employee within the meaning of section 23 of the *Australian Security Intelligence Organisation Act 1979*, the person is taken, after that commencement, to be an authorised person within the meaning of that section as amended by this Schedule.

(2) If, immediately before the commencement of this Schedule, a person was an authorising officer for the purposes of subsection 23(6) of the *Australian Security Intelligence Organisation Act 1979*, the person is taken, after that commencement, to be a person appointed under subsection 23(6A) of that Act as inserted by this Schedule.

80 Application and transitional—employees of the Organisation

A person who, immediately before the commencement of this Schedule, was an officer or employee of the Organisation employed under section 84 of the *Australian Security Intelligence Organisation Act 1979*, is, immediately after that commencement, taken to be employed:

(a) under subsection 84(1) of that Act as in force immediately after that commencement; and

(b) on the terms and conditions that were applicable to the person immediately before that commencement.

81 Employees of the Organisation—acquisition of property

(1) This item applies to a person who, immediately before the commencement of this Schedule, was an officer or employee of the Organisation employed under section 84 of the *Australian Security Intelligence Organisation Act 1979*.

(2) Section 84 of the *Australian Security Intelligence Organisation Act 1979*, as substituted by this Schedule, does not apply to the extent (if any) to which the operation of that section would result in the acquisition of property (within the meaning of paragraph 51(xxxi) of the Constitution) from the person otherwise than on just terms (within the meaning of that paragraph).

82 Transitional—former officers, employees or agents

If, immediately before the commencement of this Schedule, a person was a former officer, employee or agent of the Australian Security Intelligence Organisation, the person is, after that commencement, taken, for the purposes of the *Australian Security Intelligence Organisation Act 1979*, to be a former ASIO employee or former ASIO affiliate.

83 Transitional—authorisations under the *Australian Postal Corporation Act 1989*

If, immediately before the commencement of this Schedule, a person was an authorised ASIO officer within the meaning of section 90F of the *Australian Postal Corporation Act 1989*, the person is taken, after that commencement, to be an authorised ASIO officer within the meaning of that section as amended by this Schedule.

84 Transitional—delegations under the *Crimes Act 1914*

(1) This item applies to a delegation if the delegation was in force immediately before the commencement of this Schedule under section 15LH of the *Crimes Act 1914* in relation to a person referred to in paragraph (f) of the definition of ***senior officer*** in subsection 15LH(3) of that Act.

(2) The delegation has effect, after that commencement, as if the delegation had been made under that section in relation to a person referred to in that paragraph as amended by this Schedule.

85 Transitional—determinations under the *Public Interest Disclosure Act 2013*

(1) If, immediately before the commencement of this Schedule, a person is a person determined by the Director-General of ASIS under paragraph 41(3)(a) of the *Public Interest Disclosure Act 2013*, the person is taken, after that commencement, to be a person determined by the Director-General of ASIS under subsection 41(3) of that Act as substituted by this Schedule.

(2) If, immediately before the commencement of this Schedule, a person is a person determined by the Director-General of Security under paragraph 41(3)(b) of the *Public Interest Disclosure Act 2013*, the person is taken, after that commencement, to be a person determined by the Director-General of Security under subsection 41(4) of that Act as inserted by this Schedule.

86 Transitional—authorisations under the *Taxation Administration Act 1953*

If, immediately before the commencement of this Schedule, a person was an authorised ASIO officer within the meaning of paragraph 355-70(2)(b) of the *Taxation Administration Act 1953*, the person is taken, after that commencement, to be an authorised ASIO officer within the meaning of that paragraph as amended by this Schedule.

87 Transitional provisions—*Telecommunications (Interception and Access) Act 1979*

(1) If, immediately before the commencement of this Schedule, a person was a person authorised to be a certifying person under section 5AD of the *Telecommunications (Interception and Access) Act 1979*, the person is taken, after that commencement, to be a person authorised to be a certifying person under that section as amended by this Schedule.

(2) If, immediately before the commencement of this Schedule, a person was an authorizing officer for the purposes of section 12 of the *Telecommunications (Interception and Access) Act 1979*, the person is taken, after that commencement, to be an authorizing officer for the purposes of that section as amended by this Schedule.

(3) If, immediately before the commencement of this Schedule, a person was approved under section 12 of the *Telecommunications (Interception and Access) Act 1979*, the person is taken, after that commencement, to be a person approved under that section as amended by this Schedule.

(4) If, immediately before the commencement of this Schedule, a person was approved under paragraph 55(3)(c) of the *Telecommunications (Interception and Access) Act 1979* to exercise the authority conferred by warrants (or classes of warrants), the person is taken, after that commencement, to be approved under that paragraph as amended by this Schedule.

Schedule 2—Powers of the Organisation

Part 1—Amendments

Australian Security Intelligence Organisation Act 1979

1 Section 4 (definition of *certified copy*)

Repeal the definition, substitute:

certified copy means:

(a) in relation to a warrant—a copy of the warrant that has been certified in writing by the Director-General or a Deputy Director-General to be a true copy of the warrant; or

(b) in relation to an authorisation under section 27G—a copy of the authorisation that has been certified in writing by the Director-General or a Deputy Director-General to be a true copy of the authorisation; or

(c) in relation to an instrument varying or revoking a warrant or an authorisation under section 27G—a copy of the instrument that has been certified in writing by the Director-General or a Deputy Director-General to be a true copy of the instrument.

2 Before section 22

Insert:

Subdivision A—Preliminary

3 Section 22

Insert:

communication in transit means a communication (within the meaning of the *Telecommunications Act 1997*) passing over a telecommunications network (within the meaning of that Act).

4 Section 22 (definition of *computer*)

Repeal the definition, substitute:

computer means all or part of:

(a) one or more computers; or

(b) one or more computer systems; or
(c) one or more computer networks; or
(d) any combination of the above.

5 Section 22

Insert:

device includes instrument, apparatus and equipment.

enhancement equipment, in relation to a surveillance device, means equipment capable of enhancing a signal, image or other information obtained by the use of the surveillance device.

identified person warrant means a warrant issued under section 27C.

install includes attach and apply.

6 Section 22 (definition of *listening device*)

Repeal the definition, substitute:

listening device means any device capable of being used, whether alone or in conjunction with any other device, to overhear, record, monitor or listen to sounds, signals or a conversation, or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome that impairment and permit that person to hear only sounds ordinarily audible to the human ear.

7 Section 22

Insert:

maintain, in relation to a surveillance device, includes adjust, improve, relocate, repair, service and replace the device.

object means:
(a) a vehicle, aircraft, vessel or other means of transportation; or
(b) clothing or any other thing worn; or
(c) any other thing.

optical surveillance device means any device capable of being used, whether alone or in conjunction with any other device, to

record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

prejudicial activities of a person means activities prejudicial to security that the person is engaged in, or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in.

surveillance device means:

(a) a listening device, an optical surveillance device or a tracking device; or

(b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a) or (c); or

(c) a device of a kind prescribed by regulation for the purposes of this paragraph.

surveillance device warrant means a warrant issued under section 26.

track an object or person means be aware of the movement of the object or person from place to place.

tracking device means a device or substance that, when installed in or on an object, enables a person to track the object or a person using or wearing the object.

use of a surveillance device includes use of the device:

(a) to listen to, record, observe or monitor the words, sounds or signals communicated to or by a person, or the activities of a person; or

(b) to track an object or person.

8 Section 24

Repeal the section, substitute:

24 Exercise of authority under warrant etc.

Who may exercise authority under warrant etc.

(1) The authority conferred by a relevant warrant or relevant device recovery provision may be exercised on behalf of the Organisation only by:
  (a) the Director-General; or
  (b) a person approved under subsection (2); or
  (c) a person included in a class of persons approved under subsection (2).

Approval of persons authorised to exercise authority under warrant etc.

(2) The Director-General or a person appointed under subsection (3) may, in writing, approve a person, or a class of persons, as people authorised to exercise, on behalf of the Organisation, the authority conferred by relevant warrants or relevant device recovery provisions.

(3) The Director-General may, in writing, appoint a senior position-holder, or a class of senior position-holders, for the purposes of subsection (2).

Definitions

(4) In this section:

relevant device recovery provision means subsection 26B(5) or (6), 27A(3A) or (3B) or 27F(5).

relevant warrant means a warrant issued under this Division or under Division 3.

9 Before section 25

Insert:

Subdivision B—Search warrants

10 After paragraph 25(4)(a)

Insert:

(aa) entering any premises for the purposes of gaining entry to or exiting the subject premises;

11 Paragraph 25(5)(a)

After "adding,", insert "copying,".

12 Subsection 25(6)

Repeal the subsection, substitute:

Certain acts not authorised

(6) Subsection (5) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified under subsection (5); or

(b) cause any other material loss or damage to other persons lawfully using the computer, equipment or device.

13 Subsection 25(7) (heading)

Repeal the heading, substitute:

Warrant must provide for certain matters

14 Paragraph 25(7)(a)

After "any force", insert "against persons and things".

15 Before section 25A

Insert:

Subdivision C—Computer access warrants

16 Subsection 25A(2)

Omit "particular".

17 At the end of subsection 25A(2)

Add:

Note: See section 22 for the definition of ***computer***.

18 Subsection 25A(3)

Repeal the subsection, substitute:

(3) The target computer may be any one or more of the following:

(a) a particular computer;

(b) a computer on particular premises;

(c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

Authorisation in warrant

(3A) The warrant must:

(a) be signed by the Minister; and

(b) authorise the Organisation to do specified things, subject to any restrictions or conditions specified in the warrant, in relation to the target computer; and

(c) if the target computer is or includes a particular computer—specify the computer; and

(d) if the target computer is or includes a computer on particular premises—specify the premises; and

(e) if the target computer is or includes a computer associated with, used by or likely to be used by, a person—specify the person (whether by name or otherwise).

19 After paragraph 25A(4)(aa)

Insert:

(aaa) entering any premises for the purposes of gaining entry to or exiting the specified premises;

20 Subparagraph 25A(4)(a)(i)

Omit "a computer", substitute "the target computer".

21 Paragraph 25A(4)(a)

After "access to data", insert "(the ***relevant data***)".

22 Paragraph 25A(4)(a)

After "adding,", insert "copying,".

23 After paragraph 25A(4)(a)

Insert:

(ab) if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so—using any other computer or a communication in transit to access the relevant data and, if necessary to achieve that purpose, adding, copying, deleting or altering other data in the computer or the communication in transit;

24 Subsection 25A(4) (note)

Omit "the target computer etc.", substitute "a computer etc.".

25 Subsection 25A(5)

Repeal the subsection, substitute:

Certain acts not authorised

(5) Subsection (4) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or

(b) cause any other material loss or damage to other persons lawfully using a computer.

26 Subsection 25A(5A) (heading)

Repeal the heading, substitute:

Warrant must provide for certain matters

27 Paragraph 25A(5A)(a)

After "any force", insert "against persons and things".

28 Paragraph 25A(5A)(b)

Before "state whether", insert "if the warrant authorises entering premises—".

29 Sections 26 to 26C

Repeal the sections, substitute:

Subdivision D—Use of surveillance devices

26 Issue of surveillance device warrants

Issue of surveillance device warrant

(1) If the Director-General requests the Minister to do so, and the Minister is satisfied as mentioned in subsection (3), the Minister may issue a warrant in accordance with this section.

(2) The warrant may be issued:
  (a) in relation to one or more of the following:
    (i) a particular person;
    (ii) particular premises;
    (iii) an object or class of object; and
  (b) in respect of more than one kind of surveillance device; and
  (c) in respect of more than one surveillance device of any particular kind.

Test for issue of warrant

(3) The Minister is only to issue the warrant if he or she is satisfied that:
  (a) if the warrant is requested in relation to a particular person:
    (i) the person is engaged in or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
    (ii) the use by the Organisation of a surveillance device in relation to that person will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security; and
  (b) if the warrant is requested in relation to particular premises:
    (i) those premises are used, likely to be used or frequented by a person engaged in or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and

(ii) the use on behalf of the Organisation of a surveillance device in or on those premises will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security; and

(c) if the warrant is requested in relation to an object or class of object:

(i) that object, or an object of that class, is used or worn, or likely to be used or worn by a person engaged in or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and

(ii) the use by the Organisation of a surveillance device in or on that object, or an object of that class, will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relevant to security.

(4) To avoid doubt, the identity of the person referred to in paragraph (3)(a) or subparagraph (3)(b)(i) or (c)(i) need not be known.

Warrant may be subject to restrictions or conditions

(5) The warrant is subject to any restrictions or conditions specified in it.

26A Requirements for surveillance device warrants

(1) A surveillance device warrant must:

(a) be signed by the Minister; and

(b) specify:

(i) the kind of surveillance device, or kinds of surveillance devices, authorised to be used; and

(ii) the date the warrant is issued; and

(iii) if the warrant is issued in relation to a particular person—the name of the person (if known) or the fact that the person's identity is unknown; and

(iv) if the warrant is issued in relation to particular premises—the premises; and

(v) if the warrant is issued in relation to an object or class of object—the object or class of object; and

(c) authorise the use of any force against persons and things that is necessary and reasonable to do the things authorised by the warrant; and

(d) state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

(2) If a surveillance device warrant is issued in relation to particular premises that are vehicles, the warrant need only specify the class of vehicle in relation to which the use of the surveillance device is authorised.

(3) The surveillance device warrant must specify the period during which it is to remain in force. The period must not be more than 6 months, although the Minister may revoke the warrant before the period has expired.

(4) Subsection (3) does not prevent the issue of any further warrant.

26B What a surveillance device warrant authorises

Authorisation in warrant—particular person

(1) If a surveillance device warrant is issued in relation to a particular person, the warrant authorises the following:

(a) the installation, use and maintenance of a surveillance device of the kind specified in the warrant to:

(i) listen to, record, observe or monitor the words, sounds or signals communicated to or by the person, or the activities of the person; or

(ii) track the person;

(b) the installation, use and maintenance of a surveillance device of the kind specified in the warrant:

(i) in or on premises where the person is reasonably believed to be or likely to be; or

(ii) in or on any other premises specified in the warrant from which the activities of that person, or the words, sounds or signals communicated by or to that person, can be listened to, recorded, observed or monitored;

(c) entering the premises referred to in paragraph (b) for any of the purposes referred to in paragraph (a) or (b) or in subsection (4) or (5);

(d) the installation, use and maintenance of a surveillance device of the kind specified in the warrant in or on any object used or worn, or likely to be used or worn, by the person;

(e) the entry into or onto, or the alteration of, the object referred to in paragraph (d);

(f) entering any premises in which the object referred to in paragraph (d) is or is likely to be found, for any of the purposes referred to in that paragraph or in subsection (4) or (5);

(g) entering any other premises, for the purposes of gaining entry to or exiting premises referred in to paragraph (b) or (f);

(h) any other thing reasonably incidental to any of the above.

Authorisation in warrant—particular premises

(2) If a surveillance device warrant is issued in relation to particular premises (the ***subject premises***), the warrant authorises the following:

(a) the installation, use and maintenance of a surveillance device of the kind specified in the warrant:

(i) in or on the subject premises; or

(ii) in or on any other premises specified in the warrant from which the activities of a person, or the words, sounds or signals communicated by or to a person, can be listened to, recorded, observed or monitored while the person is in or on the subject premises;

(b) entering the subject premises, or any other premises specified in the warrant, for any of the purposes referred to in paragraph (a) or subsection (4) or (5);

(c) entering any other premises, for the purposes of gaining entry to or exiting the subject premises or any other premises specified in the warrant;

(d) any other thing reasonably incidental to any of the above.

Authorisation in warrant—object or class of object

(3) If a surveillance device warrant is issued in relation to an object, or class of object, the warrant authorises the following:

(a) the installation, use and maintenance of a surveillance device of the kind specified in the warrant in or on the specified object, or an object of the specified class;
(b) the entry into or onto, or alteration of, the specified object, or an object of the specified class;
(c) entering any premises where the object, or an object of the class, is reasonably believed to be or is likely to be for any of the purposes referred to in paragraph (a) or (b) or subsection (4) or (5);
(d) entering any other premises, for the purposes of gaining entry to or exiting premises referred to in paragraph (c);
(e) any other thing reasonably incidental to any of the above.

Authorisation in warrant—general

(4) A surveillance device warrant also authorises the following:
(a) the installation, use and maintenance of enhancement equipment in relation to the surveillance device;
(b) the temporary removal of an object from premises for the installation or maintenance of the surveillance device or enhancement equipment and the return of the object to the premises;
(c) the replacement of an object with an equivalent object for the purposes of the installation or maintenance of the surveillance device or enhancement equipment;
(d) the breaking open of any thing for the installation or maintenance of the surveillance device or enhancement equipment;
(e) the connection of the surveillance device or enhancement equipment to any source of electricity and the use of electricity from that source to operate the device or equipment;
(f) the connection of the surveillance device or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the device or equipment;
(g) the doing of any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;
(h) any other thing reasonably incidental to any of the above.

Recovery of surveillance devices

(5) If a surveillance device is installed or used under a surveillance device warrant, the Organisation is authorised to do any of the following:

(a) recover the surveillance device or any enhancement equipment in relation to the device;

(b) enter any premises where the surveillance device is reasonably believed to be, for the purpose of recovering the device or the equipment;

(c) enter any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (b);

(d) enter into or onto, or alter, an object for the purpose of recovering the device or the equipment;

(e) replace an object with an equivalent object for the purposes of recovering the device or the equipment;

(f) break open any thing for the purpose of recovering the device or the equipment;

(g) if the device or equipment is installed in or on an object—temporarily remove the object from any place where it is situated for the purpose of recovering the device or the equipment and returning the object to that place;

(h) use a nominal amount of electricity from any source to power the device or equipment;

(i) any thing reasonably necessary to conceal the fact that any thing has been done under this subsection;

(j) use any force against persons and things that is necessary and reasonable to do any of the above;

(k) any other thing reasonably incidental to any of the above;

at the following time:

(l) at any time while the warrant is in force or within 28 days after it ceases to be in force;

(m) if the surveillance device is not recovered at a time mentioned in paragraph (l)—at the earliest time, after the 28 days mentioned in that paragraph, at which it is reasonably practicable to do the things concerned.

(6) If, for the purposes of subsection (5):

(a) the surveillance device is not recovered while the warrant is in force; and

(b) the surveillance device is a tracking device;

the Organisation is also authorised to use the surveillance device or any enhancement equipment in relation to the device solely for the purposes of the location and recovery of the device or equipment.

26C Use etc. of listening device without warrant

Either of the following (the ***first person***):

(a) an ASIO employee acting in the course of the ASIO employee's duties;

(b) an ASIO affiliate acting in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation;

may install, use or maintain a listening device without warrant for any purpose involving listening to or recording words, sounds or signals being communicated by or to another person (the ***second person***) if:

(c) the first person is the communicator of the words, sounds or signals; or

(d) the second person intends, or should reasonably expect, those words, sounds or signals to be communicated to the first person, or to a class or group of persons in which the first person is included; or

(e) the first person does so with the implied or express consent of a person who is permitted under paragraph (c) or (d) to listen to or record the words, sounds or signals.

Note: This section does not apply to an ASIO affiliate specified in a determination under subsection 26F(1).

26D Use etc. of optical surveillance device without warrant

Either of the following:

(a) an ASIO employee acting in the course of the ASIO employee's duties;

(b) an ASIO affiliate acting in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation;

may install, use or maintain an optical surveillance device without warrant if the installation, use or maintenance of the device does not involve:

(c) entering premises without permission from the owner or occupier of the premises; or

(d) interference with any vehicle or thing without permission of the person having lawful possession or control of the vehicle or thing.

Note: This section does not apply to an ASIO affiliate specified in a determination under subsection 26F(1).

26E Use etc. of tracking device without warrant

(1) Either of the following:

(a) an ASIO employee acting in the course of the ASIO employee's duties;

(b) an ASIO affiliate acting in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation;

may install, use or maintain a tracking device without warrant for the purposes of tracking a person if the person consents to the installation, use or maintenance.

Note: This subsection does not apply to an ASIO affiliate specified in a determination under subsection 26F(1).

(2) Either of the following:

(a) an ASIO employee acting in the course of the ASIO employee's duties;

(b) an ASIO affiliate, acting in accordance with the contract, agreement or other arrangement under which the ASIO affiliate is performing functions or services for the Organisation;

may install, use or maintain a tracking device without warrant for the purposes of tracking an object if the person using the object consents to the installation, use or maintenance.

Note: This subsection does not apply to an ASIO affiliate specified in a determination under subsection 26F(1).

26F Director-General may determine that certain provisions do not apply to specified ASIO affiliates

(1) The Director-General may, by signed writing, determine that section 26C or 26D or subsection 26E(1) or (2) does not apply to:
  (a) a specified ASIO affiliate; or
  (b) a specified class of ASIO affiliates.

(2) A determination under subsection (1) has effect accordingly.

(3) A determination under subsection (1) is not a legislative instrument.

(4) The Director-General may, by signed writing, delegate the Director-General's power under this section to:
  (a) a Deputy Director-General; or
  (b) any other ASIO employee or ASIO affiliate who holds, or is acting in, a position in the Organisation that is equivalent to or higher than a position occupied by an SES employee with a classification of SES Band 2.

(5) In exercising powers under a delegation, the delegate must comply with any written direction given by the Director-General to the delegate.

30 Before section 27

Insert:

Subdivision E—Inspection of postal and other articles

31 Subsection 27(1)

Omit "this section or section 27A", substitute "this Division".

32 Before section 27A

Insert:

Subdivision F—Foreign intelligence

33 Paragraph 27A(1)(a)

Omit "computer or a thing", substitute "computer or an object".

34 Paragraph 27A(1)(a)

Omit "26(3) or (4), 26B(3), 26C(3)", substitute "26B(1), (2), (3) or (4)".

35 Subsection 27A(1)

Omit "those things", substitute "those objects".

36 Paragraph 27A(2)(a)

After "any force", insert "against persons and things".

37 Paragraph 27A(2)(b)

Before "state whether", insert "if the warrant authorises entering premises—".

38 Paragraph 27A(3)(b)

Omit "26(3) or (4), 26B(3), 26C(3)", substitute "26B(1), (2), (3) or (4)".

39 Subsections 27A(3A) and (3B)

Repeal the subsections, substitute:

(3A) If a surveillance device is installed or used in accordance with a warrant under this section authorising the doing of acts referred to in subsection 26B(1) (2), (3) or (4), the Organisation is authorised to do any of the following:

(a) recover the surveillance device or any enhancement equipment in relation to the device;

(b) enter any premises where the surveillance device is reasonably believed to be, for the purpose of recovering the device or the equipment;

(c) enter any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (b);

(d) enter into or onto, or alter, an object for the purpose of recovering the device or the equipment;

(e) replace an object with an equivalent object for the purposes of recovering the device or the equipment;

(f) break open any thing for the purpose of recovering the device or the equipment;

(g) if the device or equipment is installed in or on an object—temporarily remove the object from any place where it is

situated for the purpose of recovering the device or the equipment and returning the object to that place;

(h) use a nominal amount of electricity from any source to power the device or equipment;

(i) any thing reasonably necessary to conceal the fact that any thing has been done under this subsection;

(j) use any force against persons and things that is necessary and reasonable to do any of the above;

(k) any other thing reasonably incidental to any of the above;

at the following time:

(l) at any time while the warrant is in force or within 28 days after it ceases to be in force;

(m) if the surveillance device is not recovered at a time mentioned in paragraph (l)—at the earliest time, after the 28 days mentioned in that paragraph, at which it is reasonably practicable to do the things concerned.

(3B) If, for the purposes of subsection (3A):

(a) the surveillance device is not recovered while the warrant is in force; and

(b) the surveillance device is a tracking device;

the Organisation is also authorised to use the surveillance device or any enhancement equipment in relation to the device solely for the purposes of the location and recovery of the device or equipment.

40 Subsection 27A(5)

Repeal the subsection.

41 After section 27B

Insert:

Subdivision G—Identified person warrants

27C Issue of identified person warrants

Issue of warrant

(1) If the Director-General requests the Minister to do so, and the Minister is satisfied as mentioned in subsection (2), the Minister

may issue an identified person warrant in relation to a particular person.

Test for issue of warrant

(2) The Minister is only to issue an identified person warrant in relation to the person if he or she is satisfied that:
  (a) the person is engaged in or is reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security; and
  (b) the issuing of the warrant in relation to the person will, or is likely to, substantially assist the collection of intelligence relevant to security.

Requirements for warrant

(3) The identified person warrant must:
  (a) be signed by the Minister; and
  (b) identify the person:
    (i) if the name of the person is known—by specifying the person's name; or
    (ii) otherwise—by including other details sufficient to identify the person; and
  (c) give conditional approval for the Organisation to do one or more of the following:
    (i) access records or other things in or on premises;
    (ii) access data held in computers;
    (iii) use one or more kinds of surveillance devices;
    (iv) access postal articles that are in the course of the post;
    (v) access articles that are being delivered by a delivery service provider.

Note: Conditional approval does not, of itself, authorise the Organisation to do things under an identified person warrant. Things can only be done under the warrant if the Organisation is subsequently authorised to do those things: see sections 27D to 27H.

Duration of warrant

(4) An identified person warrant must specify the period during which it is to remain in force. The period must not be more than 6

months, although the Minister may revoke the warrant before the period has expired.

Issue of further warrants not prevented

(5) Subsection (4) does not prevent the issue of any further warrant.

Warrant may be subject to restrictions or conditions

(6) An identified person warrant is subject to any restrictions or conditions specified in it.

27D Authority under identified person warrant—search of premises and persons

(1) This section applies if an identified person warrant in relation to a person (the ***identified person***) gives conditional approval for the Organisation to access records or other things in or on premises.

Things that may be authorised under warrant

(2) Subject to subsection (3), the Minister or the Director-General may, on request, authorise the Organisation to do one or more of the following things under the identified person warrant in relation to one or more specified premises (the ***subject premises***):
   (a) enter the subject premises;
   (b) enter any premises for the purposes of gaining entry to or exiting the subject premises;
   (c) search the subject premises for the purpose of finding records or other things relevant to the prejudicial activities of the identified person;
   (d) open any safe, box, drawer, parcel, envelope or other container in or on the premises in which there is reasonable cause to believe that records or other things relevant to the prejudicial activities of the identified person may be found;
   (e) conduct an ordinary search or a frisk search of the identified person or any other person if:
      (i) the person is at or near the subject premises when the authority given by this subsection is exercised; and
      (ii) there is reasonable cause to believe that the person has, on his or her person, records or other things that are

relevant to the prejudicial activities of the identified person;

(f) inspect or otherwise examine any records or other things so found, and make copies or transcripts of any such record or other thing that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act;

(g) remove and retain any record or other thing so found, for the purposes of:

(i) inspecting or examining it; and

(ii) making copies or transcripts of it;

(h) if there is reasonable cause to believe that data relevant to the prejudicial activities of the identified person may be accessible by using a computer or other electronic equipment, or a data storage device, brought to or found on the subject premises—use the computer, equipment or device for the purpose of obtaining access to any such data and, if necessary to achieve that purpose, add, copy, delete or alter other data in the computer, equipment or device;

(i) if paragraph (h) applies—use the computer, equipment or device to do any of the following:

(i) inspect and examine any data to which access has been obtained;

(ii) convert any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act, into documentary form and removing any such document;

(iii) copy any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act, to any data storage device and remove the device;

(j) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;

(k) any other thing reasonably incidental to any of the above.

Test for authorisation

(3) The Minister or the Director-General is only to give an authorisation under subsection (2) if the Minister or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant in relation to the

subject premises will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

Additional rules applying to authorisations

(4) An ordinary search or frisk search of a person that is authorised under paragraph (2)(e) must, if practicable, be conducted by a person of the same sex as the person being searched.

(5) A record or other thing retained as mentioned in paragraph (2)(g) may be retained:
  (a) if returning the record or thing would be prejudicial to security—only until returning the record or thing would no longer be prejudicial to security; and
  (b) otherwise—for only such time as is reasonable.

Certain acts not authorised

(6) Paragraph (2)(e) does not authorise a strip search or a search of a person's body cavities.

(7) Paragraphs (2)(h) to (k) do not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:
  (a) materially interfere with, interrupt or obstruct the lawful use by other persons of a computer or other electronic equipment, or a data storage device, found on the subject premises unless the addition, deletion or alteration, or the doing of the thing, is necessary to do the things authorised under one or more of those paragraphs; or
  (b) cause any other material loss or damage to other persons lawfully using the computer, equipment or device.

27E Authority under identified person warrant—computer access

(1) This section applies if an identified person warrant in relation to a person (the ***identified person***) gives conditional approval for the Organisation to access data held in computers.

Things that may be authorised under warrant

(2) Subject to subsection (4), the Minister or the Director-General may, on request, authorise the Organisation to do one or more of

the following things under the identified person warrant in relation to a computer (the ***target computer***):

(a) enter specified premises for the purposes of doing the things authorised under this subsection;

(b) enter any premises for the purposes of gaining entry to or exiting the specified premises;

(c) use:

(i) the target computer; or

(ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or

(iii) any other electronic equipment; or

(iv) a data storage device;

for the purpose of obtaining access to data (the ***relevant data***) that is relevant to the prejudicial activities of the identified person and is held in the target computer at any time while the authorisation is in force and, if necessary to achieve that purpose, add, copy, delete or alter other data in the target computer;

(d) if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so—use any other computer or a communication in transit for the purpose referred to in paragraph (c) and, if necessary to achieve that purpose, add, copy, delete or alter other data in the computer or the communication in transit;

(e) copy any data to which access has been obtained, that appears to be relevant to the collection of intelligence by the Organisation in accordance with this Act;

(f) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant;

(g) any other thing reasonably incidental to any of the above.

Target computer

(3) For the purposes of subsection (2), the target computer may be any one or more of the following:

(a) a particular computer;

(b) a computer on particular premises;

(c) a computer associated with, used by or likely to be used by a person (whose identity may or may not be known).

Test for authorisation

(4) The Minister or the Director-General is only to give an authorisation under subsection (2) if the Minister or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant in relation to the target computer will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

Certain acts not authorised

(5) Subsection (2) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:
(a) materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things authorised under subsection (2); or
(b) cause any other material loss or damage to other persons lawfully using a computer.

27F Authority under identified person warrant—surveillance devices

(1) This section applies if an identified person warrant in relation to a person (the ***identified person***) gives conditional approval for the Organisation to use one or more kinds of surveillance devices.

Things that may be authorised under warrant

(2) Subject to subsection (3), the Minister or the Director-General may, on request, authorise the Organisation to do one or more of the following things under the identified person warrant:
(a) install, use and maintain surveillance devices of the kind specified in the conditional approval to:
(i) listen to, record, observe or monitor the words, sounds or signals communicated to or by the identified person, or the activities of the identified person; or
(ii) track the identified person;

(b) install, use and maintain surveillance devices of the kind specified in the conditional approval:
  (i) in or on premises where the identified person is reasonably believed to be or likely to be; or
  (ii) in or on any other specified premises from which the activities of the identified person, or the words, sounds or signals communicated by or to the identified person, can be listened to, recorded, observed or monitored;
(c) enter the premises referred to in paragraph (b) for any of the purposes referred to in paragraph (a) or (b) or in subsection 26B(4), (5) or (6) (as those subsections apply because of this section);
(d) install, use and maintain surveillance devices of the kind specified in the conditional approval in or on any object used or worn, or likely to be used or worn, by the identified person;
(e) enter into or onto, or alter, an object referred to in paragraph (d);
(f) enter any premises in which an object referred to in paragraph (d) is or is likely to be found, for any of the purposes referred to in that paragraph or in subsection 26B(4), (5) or (6) (as those subsections apply because of this section);
(g) enter any other premises, for the purposes of gaining entry to or exiting premises referred to in paragraph (b) or (f);
(h) any other thing reasonably incidental to any of the above.

Test for authorisation

(3) The Minister or the Director-General is only to give an authorisation under subsection (2) if the Minister or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

(4) If an authorisation is given under subsection (2) in relation to a surveillance device, the identified person warrant under which the authorisation is given also authorises the Organisation to do the things mentioned in subsection 26B(4) in relation to the device.

(5) If the Organisation installs or uses a surveillance device under the identified person warrant, the Organisation is authorised to do the things mentioned in subsections 26B(5) and (6) in relation to the device.

(6) For the purposes of subsections (4) and (5) of this section, section 26B applies as if references in that section to a surveillance device warrant were references to an identified person warrant.

27G Authority under identified person warrant—inspection of postal articles

(1) This section applies if an identified person warrant in relation to a person (the ***identified person***) gives conditional approval for the Organisation to access postal articles while the articles are in the course of the post.

Things that may be authorised under warrant

(2) Subject to subsection (4), the Minister or the Director-General may, on request, authorise the Organisation to do one or more of the things mentioned in subsection (3) under the identified person warrant in relation to any of the following:
  (a) articles posted by or on behalf of the identified person;
  (b) articles addressed to the identified person;
  (c) articles reasonably suspected by a person authorised to exercise the authority of the Organisation under the warrant to be intended to be received by the identified person.

(3) The things are as follows:
  (a) inspect and make copies of the articles, or the covers of the articles;
  (b) open the articles;
  (c) inspect and make copies of the contents of the articles;
  (d) any other thing reasonably incidental to any of the above.

Test for authorisation

(4) The Minister or the Director-General is only to give an authorisation under subsection (2) if the Minister or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant will substantially assist

the collection of intelligence relevant to the prejudicial activities of the identified person.

Rules relating to the Australian Postal Corporation

(5) If an authorisation is given under this section, the Director-General must, as soon as practicable:
  (a) inform the Australian Postal Corporation of that fact; and
  (b) give a certified copy of the authorisation to the Australian Postal Corporation.

(6) If either of the following is revoked:
  (a) an authorisation under this section;
  (b) the identified person warrant under which the authorisation is given;

  the Director-General must:
  (c) inform the Australian Postal Corporation of that fact; and
  (d) give a certified copy of the instrument of revocation to the Australian Postal Corporation.

(7) The Australian Postal Corporation must provide all reasonable assistance to a person acting in accordance with an authorisation under this section.

Relationship with other laws

(8) Nothing in Part VIIA of the *Crimes Act 1914* or the *Australian Postal Corporation Act 1989* prohibits the doing of anything under or for the purposes of an authorisation under this section.

27H Authority under identified person warrant—inspection of delivery articles

(1) This section applies if an identified person warrant in relation to a person (the ***identified person***) gives conditional approval for the Organisation to access articles while the articles are being delivered by a delivery service provider.

Things that may be authorised under warrant

(2) Subject to subsection (4), the Minister or the Director-General may, on request, authorise the Organisation to do one or more of

the things mentioned in subsection (3) in relation to any of the following:

(a) articles posted by or on behalf of the identified person;

(b) articles addressed to the identified person;

(c) articles reasonably suspected by a person authorised to exercise the authority of the Organisation under the warrant to be intended to be received by the identified person.

(3) The things are as follows:

(a) inspect and make copies of the articles, or the covers of the articles;

(b) open the articles;

(c) inspect and make copies of the contents of the articles;

(d) any other thing reasonably incidental to any of the above.

Test for authorisation

(4) The Minister or the Director-General is only to give an authorisation under subsection (2) if the Minister or the Director-General is satisfied, on reasonable grounds, that doing that thing or those things under the warrant will substantially assist the collection of intelligence relevant to the prejudicial activities of the identified person.

Definitions

(5) In this section:

article has the same meaning as in section 27AA.

delivery service provider has the same meaning as in section 27AA.

27J Authority under identified person warrants—general rules

Requests for authorisations

(1) A request for an authorisation under this Subdivision may be made:

(a) if the request is to the Minister—by the Director-General; or

(b) if the request is to the Director-General—by an ASIO employee or an ASIO affiliate.

(2) The request must specify the facts and other grounds on which the person making the request considers it necessary that the authorisation should be given.

Requirements for authorisations

(3) An authorisation under this Subdivision:
  (a) must be in writing; and
  (b) must identify the identified person warrant under which the authorisation is given; and
  (c) must specify:
    (i) for an authorisation under section 27D (search of premises or persons)—the subject premises; and
    (ii) for an authorisation under section 27E (computer access)—the target computer; and
    (iii) the thing or things that are authorised to be done; and
    (iv) the restrictions or conditions (if any) to which the authorisation is subject; and
    (v) the period during which the authorisation is in force; and
  (d) must authorise the use of any force against persons and things that is necessary and reasonable to do the things covered by the authorisation; and
  (e) if the authorisation authorises entering premises—must state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

(4) A restriction or condition specified in an authorisation must not be inconsistent with any restrictions or conditions specified in the identified person warrant under which the authorisation is given.

(5) For the purposes of subparagraph (3)(c)(v), the period:
  (a) in the case of an authorisation under section 27D (search of premises and persons)—must not be more than 90 days; and
  (b) in any case—must not end after the end of the period for which the identified person warrant under which the authorisation is given is in force.

When authorisations cease to be in force

(6) An authorisation under this Subdivision ceases to be in force at the earliest of the following times:
  (a) the time the identified person warrant under which the authorisation is given ceases to be in force;
  (b) the time it is revoked by the Minister or the Director-General;
  (c) the time specified in the authorisation.

Other matters

(7) To avoid doubt, for the purposes of this Act, the authority conferred by an identified person warrant includes the authority conferred by an authorisation under this Subdivision under the warrant.

(8) To avoid doubt, nothing in this Subdivision prevents 2 or more authorisations under this Subdivision from being given under the same identified persons warrant at any time while the warrant is in force.

(9) An authorisation under this Subdivision is not a legislative instrument.

42 Before section 28

Insert:

Subdivision H—General provisions relating to warrants

43 Paragraph 29(1)(a)

Omit "26B, 26C,".

44 After section 29

Insert:

29A Variation of warrants issued under this Division

(1) The Minister may, on request by the Director-General, vary a warrant issued under this Division (other than under section 29).

(2) The variation must be in writing.

(3) If the variation extends, or further extends, the period during which the warrant is in force, the total period during which the warrant is in force must not exceed:
   (a) for a warrant issued under section 25—90 days; or
   (b) for a warrant issued under section 25A, 26, 27, 27AA or 27C—6 months.

(4) The request by the Director-General must specify:
   (a) the facts and other grounds on which the Director-General considers it necessary that the warrant should be varied; and
   (b) where appropriate—the grounds on which the Director-General suspects a person of being engaged in or reasonably suspected by the Director-General of being engaged in, or of being likely to engage in, activities prejudicial to security.

(5) A warrant may be varied more than once under this section.

45 Section 30

Repeal the section, substitute:

30 Discontinuance of action before expiration of warrant

(1) Subject to subsection (3), if the Director-General is satisfied that the grounds on which a warrant under this Division was issued have ceased to exist, the Director-General must, as soon as practicable:
   (a) inform the Minister of that fact; and
   (b) take such steps as are necessary to ensure that action under the warrant is discontinued.

(2) For the purposes of paragraph (1)(b), ***action under a warrant***:
   (a) includes action under an authorisation given under an identified person warrant; but
   (b) does not include the recovery of a surveillance device or any enhancement equipment in relation to the device.

(3) If:
   (a) a surveillance device warrant was issued in relation to more than one of the matters mentioned in paragraph 26(2)(a); and

(b) the grounds on which the warrant was issued continue to exist for at least one of those matters;

subsection (1) applies only in relation to the matters for which the grounds have ceased to exist.

45A After section 31

Insert:

31A Notification requirements in relation to the use of force under warrant

(1) This section applies if a warrant issued under this Division authorises the use of force against persons to do the things authorised by the warrant.

(2) The Director-General must cause the Minister and the Inspector-General of Intelligence and Security to be notified if such force is used against a person in the execution of the warrant.

(3) The notification must be given:

(a) in writing; and

(b) as soon as practicable after such force is used.

46 After section 32

Insert:

33 Relationship with other laws

Computer access—relationship with the Telecommunications (Interception and Access) Act 1979

(1) Nothing in section 25A, 27A or 27E, or in a warrant or authorisation under those sections, authorises, for the purposes of the *Telecommunications (Interception and Access) Act 1979*, the interception of a communication passing over a telecommunications system operated by a carrier or a carriage service provider.

Listening devices—relationship with the Telecommunications (Interception and Access) Act 1979

(2) Nothing in section 26B, 27A or 27F, or in a warrant or authorisation under those sections, applies to or in relation to the use of a listening device for a purpose that would, for the purposes of the *Telecommunications (Interception and Access) Act 1979*, constitute the interception of a communication passing over a telecommunications system operated by a carrier or a carriage service provider.

Surveillance devices—interaction with other laws

(3) Despite any other law of the Commonwealth, a State or a Territory (including the common law), a person acting on behalf of the Organisation does not act unlawfully by installing, using or maintaining a surveillance device if the person does so:
  (a) in accordance with a warrant issued under section 26, 27A or 27C; or
  (b) in accordance with subsection 26B(5) or (6), section 26C, 26D, or 26E, or subsection 27A(3A) or (3B) or 27F(5).

46A Section 34

Before "The", insert "(1)".

46B At the end of section 34

Add:

(2) If:
  (a) the warrant was issued under section 25, 25A, 27A, 27C or 29; and
  (b) a thing mentioned in subsection 25(5) or 25A(4), paragraph 27D(2)(h) to (k) or subsection 27E(2) was done under the warrant;

the report must also include details of anything done that materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or other electronic equipment, or a data storage device.

47 At the end of Division 2 of Part III

Add:

34AA Evidentiary certificates

(1) Subject to subsection (2), the Director-General or a Deputy Director-General may issue a written certificate setting out such facts as he or she considers relevant with respect to acts or things done by, on behalf of, or in relation to, the Organisation:
  (a) in connection with a relevant warrant; or
  (b) in accordance with a relevant authorising provision.

(2) A certificate may be issued with respect to acts or things done in connection with:
  (aa) a warrant issued under section 25, but only if the warrant authorises the doing of acts or things referred to in paragraph 25(5)(a), (b), (c) or (d), and only with respect to those acts or things; or
  (a) a warrant issued under section 27A or 29, but only if the warrant authorises the doing of acts or things referred to in subsection 25(5) or section 25A or 26B, and only with respect to those acts or things; or
  (b) a warrant issued under section 27C, but only if acts or things are authorised under paragraphs 27D(2)(h) to (k) or section 27E or 27F under the warrant, and only with respect to those acts or things.

(3) Without limiting subsection (1), the certificate may set out one or more of the following:
  (a) if premises were entered under the relevant warrant or relevant authorising provision:
    (i) details of the premises; or
    (ii) the time of day or night the premises were entered;
  (b) if data was accessed under the relevant warrant or relevant authorising provision—details of the computer, telecommunications facility, electronic equipment, data storage device or communication in transit used for the purpose of obtaining such access;
  (c) if the warrant is a surveillance device warrant—the matters required to be specified under section 26A for the warrant;
  (d) if one or more surveillance devices were installed, used or maintained under the relevant warrant or relevant authorising provision:

(i) details of the installation, use or maintenance of the surveillance device or devices; or

(ii) details of the installation, use or maintenance of any enhancement equipment in relation to the surveillance device; or

(iii) details of the processes and procedures employed to use the surveillance device or devices, or any enhancement equipment; or

(iv) details of acts or things done for the purposes of recovering the surveillance device or devices, or any enhancement equipment;

(e) details of things done under the relevant warrant or relevant authorising provision that were reasonably necessary to conceal the fact that things were done under the relevant warrant or relevant authorising provision;

(f) details of persons who exercised the authority given by the relevant warrant or relevant authorising provision;

(g) details of things done under the relevant warrant or relevant authorising provision that were reasonably incidental to any of the acts or things done by, on behalf of, or in relation to, the Organisation in connection with the relevant warrant or relevant authorising provision.

(4) In a proceeding, a certificate under subsection (1) is prima facie evidence of the matters stated in the certificate.

(5) In this section:

proceeding means:

(a) a proceeding or proposed proceeding in a federal court, or in a court of a State or Territory; or

(b) a proceeding or proposed proceeding (including a hearing or examination, or proposed hearing or examination) by or before:

(i) a tribunal in Australia; or

(ii) any other body, authority or person in Australia having power to hear or examine evidence.

relevant authorising provision means subsection 26B(5) or (6), section 26C, 26D or 26E or subsection 27A(3A) or (3B) or 27F(5).

relevant warrant means a warrant issued under section 25, 25A, 26, 27A, 27C or 29.

Part 2—Consequential amendments

Telecommunications (Interception and Access) Act 1979

48 After paragraph 108(2)(c)

Insert:

(ca) accessing a stored communication under an authorisation given under a warrant in accordance with section 27E of the *Australian Security Intelligence Organisation Act 1979*; or

49 At the end of paragraph 108(2)(f)

Add:

(iv) authorisations given under warrants in accordance with section 27E of the *Australian Security Intelligence Organisation Act 1979*; or

Part 3—Application, transitional and savings provisions

50 Application, transitional and savings provisions

(1) Subject to this item, the amendments made by this Schedule do not apply in relation to:

(a) warrants requested before the commencement of this Schedule; or

(b) warrants issued before the commencement of this Schedule.

(2) If, immediately before the commencement of this Schedule, a person was approved under subsection 24(1) of the *Australian Security Intelligence Organisation Act 1979*, the person is taken, after that commencement, to be a person approved under subsection 24(2) of that Act as amended by this Schedule.

(3) If, immediately before the commencement of this Schedule, a person was an authorising officer for the purposes of subsection 24(1) of the *Australian Security Intelligence Organisation Act 1979*, the person is taken, after that commencement, to be a person appointed under subsection 24(3) of that Act as amended by this Schedule.

(4) Section 34AA of the *Australian Security Intelligence Organisation Act 1979*, as inserted by this Schedule, applies in relation to:

(a) warrants issued, and authorisations given, after the commencement of this Schedule; and

(b) proceedings commenced after that commencement.

Schedule 3—Protection for special intelligence operations

Australian Security Intelligence Organisation Act 1979

1 Section 4

Insert:

engage in conduct has the same meaning as in the *Criminal Code*.

IGIS official (short for Inspector-General of Intelligence and Security official) means:

(a) the Inspector-General of Intelligence and Security; or

(b) a member of the staff referred to in subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*.

participant in a special intelligence operation means a person who is authorised under Division 4 of Part III to engage in special intelligence conduct for the purposes of the special intelligence operation.

special intelligence conduct means conduct for or in relation to which a person would, but for section 35K, be subject to civil or criminal liability under a law of the Commonwealth, a State or a Territory.

special intelligence function means a function of the Organisation under paragraph 17(1)(a), (b), (e) or (f).

special intelligence operation is an operation:

(a) in relation to which a special intelligence operation authority has been granted; and

(b) that is carried out for a purpose relevant to the performance of one or more special intelligence functions; and

(c) that may involve an ASIO employee or an ASIO affiliate in special intelligence conduct.

special intelligence operation authority means an authority to conduct a special intelligence operation granted under section 35C.

2 Subsection 34ZF(8)

Repeal the subsection.

3 At the end of Part III

Add:

Division 4—Special intelligence operations

35A Relationship to other laws and matters

(1) Subject to subsection (2) and section 35R, this Division is not intended to limit a discretion that a court has:

(a) to admit or exclude evidence in any proceedings; or

(b) to stay criminal proceedings in the interests of justice.

(2) In determining whether evidence should be admitted or excluded in any proceedings, the fact that the evidence was obtained as a result of a person engaging in criminal activity is to be disregarded if:

(a) the person was a participant in a special intelligence operation authorised under this Division acting in the course of the special intelligence operation; and

(b) the criminal activity was special intelligence conduct.

35B Applications for authorities to conduct special intelligence operations

(1) The Director-General, a senior position-holder or an ASIO employee may apply to the Minister for an authority to conduct a special intelligence operation on behalf of the Organisation.

(2) An application may be made:

(a) in writing signed by the applicant; or

(b) if the applicant reasonably believes that the delay caused by making a written application may be prejudicial to security—orally in person, or by telephone or other means of communication.

(3) To avoid doubt, nothing in this Division prevents an application for a special intelligence operation authority being made in respect of a special intelligence operation that has been the subject of a previous application.

Note: A special intelligence operation authority can be varied, but not so as to extend beyond 12 months—see section 35F.

(4) As soon as practicable after making an application in accordance with paragraph (2)(b), the applicant must:
  (a) make a written record of the application; and
  (b) give a copy of it to the Minister.

35C Granting of special intelligence operation authorities

(1) If:
  (a) an application for an authority to conduct a special intelligence operation is made under section 35B; and
  (b) the Minister is satisfied that there are reasonable grounds on which to believe that the matters in subsection (2) exist;

the Minister may authorise the special intelligence operation by granting the authority.

(2) The matters are as follows:
  (a) the special intelligence operation will assist the Organisation in the performance of one or more special intelligence functions;
  (b) the circumstances are such as to justify the conduct of a special intelligence operation;
  (c) any unlawful conduct involved in conducting the special intelligence operation will be limited to the maximum extent consistent with conducting an effective special intelligence operation;
  (d) the special intelligence operation will not be conducted in such a way that a person is likely to be induced to commit an offence against a law of the Commonwealth, a State or a Territory that the person would not otherwise have intended to commit;
  (e) any conduct involved in the special intelligence operation will not:
    (i) cause the death of, or serious injury to, any person; or
    (ia) constitute torture; or
    (ii) involve the commission of a sexual offence against any person; or

(iii) result in significant loss of, or serious damage to, property.

(3) A special intelligence operation authority may be granted unconditionally or subject to conditions.

(4) A special intelligence operation authority may be granted:

(a) by means of a written document signed by the Minister; or

(b) if the Minister is satisfied there are reasonable grounds on which to believe that the delay caused by giving a written authority may be prejudicial to security—orally in person, or by telephone or other means of communication.

(5) If a special intelligence operation authority is granted in accordance with paragraph (4)(b), a written record of the special intelligence operation authority that complies with section 35D must be issued within 7 days.

(6) To avoid doubt, nothing in this Division prevents a special intelligence operation authority being granted in respect of a special intelligence operation that has been the subject of a previous special intelligence operation authority.

Note: A special intelligence operation authority can be varied, but not so as to extend beyond 12 months—see section 35F.

(7) The following are not legislative instruments:

(a) a document referred to in paragraph (4)(a);

(b) a written record referred to in subsection (5).

35D Contents of special intelligence operation authorities

(1) A special intelligence operation authority must:

(a) state how the special intelligence operation will assist the Organisation in the performance of one or more special intelligence functions; and

(b) identify the persons authorised to engage in special intelligence conduct for the purposes of the special intelligence operation; and

(c) state a description of the nature of the special intelligence conduct that the persons referred to in paragraph (b) may engage in; and

(d) specify the period of effect of the special intelligence operation authority, being a period not exceeding 12 months; and

(e) specify any conditions to which the conduct of the special intelligence operation is subject; and

(f) state the date and time when the special intelligence operation authority is granted.

(2) A person is sufficiently identified for the purposes of paragraph (1)(b) if the person is identified:

(a) by an assumed name under which the person is operating; or

(b) by a code name or code number;

as long as the person's identity can be matched to the assumed name, code name or code number.

35E Commencement and duration of special intelligence operation authorities

(1) A special intelligence operation authority comes into force at the time the special intelligence operation authority is granted under section 35C.

(2) A special intelligence operation authority has effect for the period specified in accordance with paragraph 35D(1)(d) unless:

(a) it is cancelled before the end of the period of effect; or

(b) the period of effect is extended under section 35F.

35F Variation of special intelligence operation authorities

(1) The Minister may vary a special intelligence operation authority on application by the Director-General, a senior position-holder or an ASIO employee.

Application for variation

(2) An application under subsection (1) may be made:

(a) in writing signed by the applicant; or

(b) if the applicant reasonably believes that the delay caused by making a written application may be prejudicial to security—orally in person, or by telephone or other means of communication.

(3) As soon as practicable after making an application in accordance with paragraph (2)(b), the applicant must:
  (a) make a written record of the application; and
  (b) give a copy of it to the Minister.

Limits on variation

(4) The Minister must not vary the special intelligence operation authority unless the Minister:
  (a) is satisfied that there are reasonable grounds on which to believe that the special intelligence operation, conducted in accordance with the special intelligence operation authority as varied, will assist the Organisation in the performance of one or more special intelligence functions; and
  (b) considers it is appropriate to do so.

(5) If a variation extends, or further extends, the period of effect of a special intelligence operation authority, the total period of effect must not be longer than 12 months.

Manner of variation

(6) The variation may be made:
  (a) by means of a written document signed by the Minister; or
  (b) if the Minister is satisfied there are reasonable grounds on which to believe that the delay caused by giving a written variation may be prejudicial to security—orally in person, or by telephone or other means of communication.

(7) If a special intelligence operation authority is varied in accordance with paragraph (6)(b), a written record of the variation must be issued within 7 days.

Authority may be varied more than once

(8) A special intelligence operation authority may be varied more than once under this section.

35G Cancellation of special intelligence operation authorities

(1) The Director-General or a Deputy Director-General may cancel a special intelligence operation authority at any time and for any reason.

(2) A cancellation of a special intelligence operation authority must:
  (a) be in writing; and
  (b) specify when the cancellation takes effect.

35H Effect of special intelligence operation authorities

(1) A special intelligence operation authority authorises each person who is identified in the special intelligence operation authority to engage in the special intelligence conduct specified in the special intelligence operation authority in respect of that person.

(2) The authorisation, in relation to a person identified in the special intelligence operation authority, is for the period of effect of the special intelligence operation authority, unless:
  (a) the special intelligence operation authority specifies a shorter period during which the person is so authorised; or
  (b) the special intelligence operation authority is varied under section 35F to provide that the person is no longer so authorised; or
  (c) the special intelligence operation authority is cancelled before the end of that period.

35J Defect in a special intelligence operation authority

An application for a special intelligence operation authority or variation of such an authority, and any special intelligence operation authority or variation of such an authority granted on the basis of such an application, is not invalidated by any defect, other than a defect that affects the application, special intelligence operation authority or variation in a material particular.

35K Immunity from liability for special intelligence conduct during special intelligence operations

(1) A participant in a special intelligence operation is not subject to any civil or criminal liability for or in relation to conduct if:

(a) the participant engages in the conduct in the course of, and for the purposes of, the special intelligence operation; and

(b) the participant engages in the conduct in accordance with the special intelligence operation authority to conduct the special intelligence operation; and

(c) the participant is identified in the special intelligence operation authority as a person authorised to engage in special intelligence conduct for the purposes of the special intelligence operation; and

(d) the conduct does not involve the participant intentionally inducing another person to commit an offence against a law of the Commonwealth, a State or a Territory that the other person would not otherwise have intended to commit; and

(e) the conduct does not involve the participant engaging in any conduct that:

(i) causes the death of, or serious injury to, any person; or

(ia) constitutes torture; or

(ii) involves the commission of a sexual offence against any person; or

(iii) causes significant loss of, or serious damage to, property; and

(f) the requirements (if any) specified in a determination under subsection (2) have been met.

(2) The Minister may, by legislative instrument, determine requirements for the purposes of paragraph (1)(f).

35L Requirements for warrants etc. not affected

(1) If, apart from this Division, the Organisation could not do a particular act without it being authorised by warrant issued under this Act or under Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*, this Division does not allow the Organisation to do the act without the warrant.

(2) If, apart from this Division, the Organisation could not obtain particular information other than in accordance with Division 3 of Part 4-1 of the *Telecommunications (Interception and Access) Act 1979*, this Division does not allow the Organisation to obtain the information otherwise than in accordance with that Division of the *Telecommunications (Interception and Access) Act 1979*.

(3) This section is enacted to avoid doubt.

35M Effect of being unaware of variation or cancellation of special intelligence operation authority

(1) If an authority to conduct a special intelligence operation is varied in a way that limits its scope, this Division continues to apply to a participant in the special intelligence operation as if the authority had not been varied in that way, for so long as the participant:
  (a) is unaware of the variation; and
  (b) is not reckless about the existence of the variation.

(2) If an authority to conduct a special intelligence operation is cancelled, this Division continues to apply to a person who was a participant in the special intelligence operation immediately before the cancellation as if the authority had not been cancelled in that way, for so long as the person:
  (a) is unaware of the cancellation; and
  (b) is not reckless about the existence of the cancellation.

(3) For the purposes of this section, a person is reckless about the existence of the variation or cancellation of a special intelligence operation authority if:
  (a) the person is aware of a substantial risk that the variation or cancellation has happened; and
  (b) having regard to the circumstances known to the person, it is unjustifiable to take the risk that the special intelligence operation authority has not been varied or cancelled.

35N Protection from criminal responsibility for certain ancillary conduct

(1) This section applies if:
  (a) a person engages in conduct (the ***ancillary conduct***) that relates to special intelligence conduct (the ***related conduct***) engaged in by another person; and
  (b) engaging in the ancillary conduct is an ancillary offence in relation to the offence constituted by the related conduct.

(2) Despite any other law of the Commonwealth, a State or a Territory, the person who engaged in the ancillary conduct is not criminally

responsible for the ancillary offence, if, at the time the person engaged in the ancillary conduct, he or she believed the related conduct was being engaged in, or would be engaged in, by a participant in a special intelligence operation authorised under this Division.

(3) For the purposes of this section, ***ancillary offence***, in relation to an offence constituted by related conduct, means an offence against a law of the Commonwealth, a State or a Territory:

(a) of conspiring to commit the offence constituted by the related conduct; or

(b) of aiding, abetting, counselling or procuring, inciting or being in any way knowingly concerned in, the commission of the offence constituted by the related conduct.

35P Unauthorised disclosure of information

Unauthorised disclosure of information

(1) A person commits an offence if:

(a) the person discloses information; and

(b) the information relates to a special intelligence operation.

Penalty: Imprisonment for 5 years.

Note: Recklessness is the fault element for the circumstance described in paragraph (1)(b)—see section 5.6 of the *Criminal Code*.

Unauthorised disclosure of information—endangering safety, etc.

(2) A person commits an offence if:

(a) the person discloses information; and

(b) the information relates to a special intelligence operation; and

(c) either:

(i) the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation; or

(ii) the disclosure of the information will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

Penalty: Imprisonment for 10 years.

Note: Recklessness is the fault element for the circumstance described in paragraph (2)(b)—see section 5.6 of the *Criminal Code*.

Exceptions

(3) Subsections (1) and (2) do not apply if the disclosure was:

(a) in connection with the administration or execution of this Division; or

(b) for the purposes of any legal proceedings arising out of or otherwise related to this Division or of any report of any such proceedings; or

(c) in accordance with any requirement imposed by law; or

(d) in connection with the performance of functions or duties, or the exercise of powers, of the Organisation; or

(e) for the purpose of obtaining legal advice in relation to the special intelligence operation; or

(f) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the *Inspector-General of Intelligence and Security Act 1986*; or

(g) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act.

Note: A defendant bears an evidential burden in relation to the matters in this subsection—see subsection 13.3(3) of the *Criminal Code*.

Extended geographical jurisdiction

(4) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to an offence against subsection (1) or (2).

(5) Subsection (4) does not, by implication, affect the interpretation of any other provision of this Act.

35PA Notifications by Director-General

(1) The Director-General must cause the Inspector-General of Intelligence and Security to be notified if a special intelligence operation is authorised under this Division.

(2) The notification must be given:

(a) in writing; and
(b) as soon as practicable after the special intelligence operation authority is granted.

35Q Reports by the Director-General

(1) If a special intelligence operation is authorised under this Division, the Director-General must give the Minister and the Inspector-General of Intelligence and Security a written report:
(a) if the special intelligence operation authority has effect for a period of 6 months or less—for that period; or
(b) otherwise:
(i) for the first 6-months during which the special intelligence operation authority has effect; and
(ii) for the remainder of the period during which the special intelligence operation authority has effect.

(2) A report under subsection (1) must report on the extent to which the special intelligence operation has, during the period to which the report relates, assisted the Organisation in the performance of one or more special intelligence functions.

Note: The Inspector-General of Intelligence and Security has oversight powers in relation to conduct engaged in accordance with this Division: see section 8 of the *Inspector-General of Intelligence and Security Act 1986*.

(2A) A report under subsection (1) must report on whether conduct of a participant in a special intelligence operation:
(a) caused the death of, or injury to, any person; or
(b) involved the commission of a sexual offence against any person; or
(c) resulted in loss of, or damage to, property.

(3) A report under subsection (1) is not a legislative instrument.

35R Evidence relating to granting of special intelligence operation authority

(1) The Minister may issue a written certificate signed by the Minister setting out such facts as the Minister considers relevant with respect to the granting of a special intelligence operation authority.

(2) In any proceeding, a certificate under subsection (1) is prima facie evidence of the matters stated in the certificate.

4 After subsection 94(2)

Insert:

(2A) A report under subsection (1) must also include a statement of:

(a) the total number of applications made under section 35B during the year for the granting of special intelligence operation authorities; and

(b) the total number of special intelligence operation authorities granted during the year.

Schedule 4—ASIO co-operation and information sharing

Australian Security Intelligence Organisation Act 1979

4 At the end of paragraph 19(1)(a)

Add "and".

5 At the end of subsection 19(1)

Add:

; and (d) any other person or body whether within or outside Australia.

6 At the end of section 92

Add:

Note: For communication of information about an offence against this section to appropriate authorities, see subsection 18(3).

Schedule 5—Activities and functions of Intelligence Services Act 2001 agencies

Intelligence Services Act 2001

1 Section 3

Insert:

operational security of ASIS means the protection of the integrity of operations undertaken by ASIS from:

(a) interference by a foreign person or entity; or

(b) reliance on inaccurate or false information.

2 Before section 6

Insert:

Division 1—Functions of the agencies

3 After paragraph 6(1)(da)

Insert:

(db) to undertake activities in accordance with section 13B; and

4 Subparagraph 6B(e)(ii)

Omit "such imagery or products", substitute "imagery and other geospatial products".

5 After subparagraph 6B(e)(ii)

Insert:

(iia) assistance in relation to the production and use of imagery and other geospatial technologies;

6 After subparagraph 9(1A)(a)(iii)

Insert:

(iiia) activities that pose a risk, or are likely to pose a risk, to the operational security of ASIS;

7 Subsection 9(1B) (note)

After "***crime***", insert "and ***operational security of ASIS***".

8 Before section 13

Insert:

Division 2—Co-operation

9 Subsection 13(1A)

Omit all the words after "planning or", substitute:

undertaking:

(a) activities covered by paragraphs 6(4)(a) to (c); or

(b) training in the use of weapons or in self-defence techniques;

unless, before giving the approval, the Minister consults with the Prime Minister and the Attorney-General.

10 Application—subsection 13(1A)

(1) The amendment of subsection 13(1A) of the *Intelligence Services Act 2001* made by this Schedule applies in relation to co-operation with an authority, in planning or undertaking training in the use of weapons or in self-defence techniques, on or after the commencement of this Schedule.

(2) Subitem (1) applies whether an approval under paragraph 13(1)(c) of the *Intelligence Services Act 2001* was given in relation to the authority before or after the commencement of this Schedule.

11 After section 13A

Insert:

Division 3—Activities undertaken in relation to ASIO

13B Activities undertaken in relation to ASIO

When an activity may be undertaken in relation to ASIO

(1) Subject to section 13D, ASIS may undertake an activity, or a series of activities, if:

(a) the activity or series of activities will be undertaken for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person or a class of Australian persons; and

(b) the activity or series of activities will be undertaken outside Australia; and

(c) the activity or series of activities will be undertaken to support ASIO in the performance of its functions; and

(d) either:

(i) the Director-General of Security; or

(ii) a person who is authorised under section 13C for the purposes of this subparagraph;

has, in writing, notified ASIS that ASIO requires the production of intelligence on the Australian person or class of Australian persons.

(2) The undertaking of an activity or series of activities under subsection (1) is subject to any conditions specified in the notice under paragraph (1)(d).

When notice from ASIO not required—particular activity

(3) Paragraph (1)(d) does not apply in relation to the undertaking of a particular activity in relation to a particular Australian person if a staff member of ASIS who:

(a) is authorised under subsection (7); and

(b) will be undertaking the activity;

reasonably believes that it is not practicable in the circumstances for ASIO to notify ASIS in accordance with that paragraph before undertaking the activity.

(4) If ASIS undertakes an activity in accordance with subsection (3), ASIS must, as soon as practicable, notify ASIO and the Inspector-General of Intelligence and Security, in writing, of the activity.

Effect of this section

(5) ASIS may undertake an activity or series of activities under subsection (1) without an authorisation under section 9 for the activity or series of activities.

Incidental production of intelligence

(6) An activity, or a series of activities, does not cease to be undertaken:
  (a) in accordance with this section; or
  (b) for the specific purpose of supporting ASIO in the performance of its functions;

only because, in undertaking the activity or series of activities, ASIS also incidentally produces intelligence that relates to the involvement, or likely involvement, of an Australian person in one or more of the activities set out in paragraph 9(1A)(a).

Authorised staff members

(7) The Director-General may authorise, in writing, a staff member of ASIS, or a class of such staff members, for the purposes of paragraph (3)(a).

Instruments not legislative instruments

(8) The following are not legislative instruments:
  (a) a notice under paragraph (1)(d);
  (b) a notice under subsection (4);
  (c) an authorisation made under subsection (7).

13C Authorised persons for activities undertaken in relation to ASIO

Authorised persons

(1) The Director-General of Security may authorise, in writing, a senior position-holder, or a class of senior position-holders, for the purposes of subparagraph 13B(1)(d)(ii).

Authorisation is not a legislative instrument

(2) An authorisation made under subsection (1) is not a legislative instrument.

Definitions

(3) For the purposes of this section, ***senior position-holder*** has the same meaning as in the *Australian Security Intelligence Organisation Act 1979*.

13D Certain acts not permitted

If ASIO could not undertake a particular act in at least one State or Territory without it being authorised by warrant under Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* or under Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*, this Division does not allow ASIS to undertake the act.

13E Director-General to be satisfied of certain matters

The Director-General must be satisfied that:

(a) there are satisfactory arrangements in place to ensure that activities will be undertaken in accordance with section 13B only for the specific purpose of supporting ASIO in the performance of its functions; and

(b) there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in accordance with section 13B will be reasonable, having regard to the purposes for which they are carried out.

13F Other matters relating to activities undertaken in relation to ASIO

ASIO to be consulted before communicating intelligence

(1) If, in undertaking an activity or series of activities in accordance with section 13B, ASIS produces intelligence, ASIS must not communicate the intelligence outside ASIS (other than in accordance with subsection (2)) unless ASIO has been consulted.

Intelligence to be communicated to ASIO

(2) If, in undertaking an activity or series of activities in accordance with section 13B, ASIS produces intelligence, ASIS must cause the

intelligence to be communicated to ASIO as soon as practicable after the production.

Notices to be made available to the Inspector-General of Intelligence and Security

(3) If a notice is given to ASIS under paragraph 13B(1)(d), the Director-General must ensure that a copy of the notice is kept by ASIS and is available for inspection on request by the Inspector-General of Intelligence and Security.

Reports about activities to be given to the responsible Minister

(4) As soon as practicable after each year ending on 30 June, the Director-General must give to the responsible Minister in relation to ASIS a written report in respect of activities undertaken by ASIS in accordance with section 13B during the year.

13G Guidelines relating to activities undertaken in relation to ASIO

(1) The responsible Minister in relation to ASIO and the responsible Minister in relation to ASIS may jointly make written guidelines relating to the undertaking of activities in accordance with section 13B.

(2) Guidelines made under subsection (1) are not a legislative instrument.

12 Before section 14

Insert:

Division 4—Other

13 Subsection 14(2)

Omit "done inside Australia", substitute "(whether done inside or outside Australia)".

14 After subclause 1(1) of Schedule 2

Insert:

(1A) The provision to a person of a weapon, or training in the use of a weapon or in self-defence techniques, is not prevented by subsection 6(4) if:

(a) the person:

(i) is an officer of an authority with which ASIS is co-operating in accordance with paragraph 13(1)(c); or

(ii) is an officer (however described) of a Commonwealth authority, or a State authority, and is authorised in that capacity to carry and use weapons; and

(b) it is provided in accordance with a Ministerial approval under subclause (3A) in relation to the person; and

(c) it is provided for the purpose of enabling the person:

(i) to protect himself or herself; or

(ii) to protect a staff member or agent of ASIS; or

(iii) to protect a person who is co-operating with ASIS in accordance with section 13.

15 Subparagraph 1(2)(a)(ii) of Schedule 2

After "(1)", insert "or (1A)".

16 After subclause 1(2) of Schedule 2

Insert:

(2A) The use of a weapon or self-defence techniques is not prevented by subsection 6(4) if:

(a) the weapon or techniques are used in the proper performance of a function of ASIS; and

(b) the weapon or techniques are used in a controlled environment; and

(c) guidelines have been issued by the Director-General under subclause (6); and

(d) the weapon or techniques are used in compliance with those guidelines.

Example: The following may constitute the use of a weapon or technique in a controlled environment:

(a) the use of a firearm at a rifle range;

(b) the use of a martial art at a martial arts club.

17 After subclause 1(3) of Schedule 2

Insert:

(3A) The Minister may, by written notice given to the Director-General, approve the provision of a weapon, or training in the use of a weapon or in self-defence techniques, to a specified person for the purposes of paragraph (1A)(b).

18 Subclause 1(4) of Schedule 2

After "An approval", insert "under subclause (3) or (3A)".

19 Subclause 1(5) of Schedule 2

After "an approval", insert "under subclause (3) or (3A)".

20 Clause 2 of Schedule 2

Omit "A staff member or agent of ASIS", substitute "A person".

Schedule 6—Protection of information

Part 1—Main amendments

Australian Security Intelligence Organisation Act 1979

1 Subsection 18(2) (penalty)

Omit "2 years", substitute "10 years".

2 After subsection 18(2)

Insert:

Exception—information or matter lawfully available

(2A) Subsection (2) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the *Criminal Code*).

Exception—communication to the Inspector-General of Intelligence and Security

(2B) Subsection (2) does not apply if the person communicates the information or matter to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2B) (see subsection 13.3(3) of the *Criminal Code*).

3 Subsection 18(5)

Repeal the subsection.

4 After section 18

Insert:

18A Unauthorised dealing with records

Offence for unauthorised dealing with records

(1) A person commits an offence if:

(a) the person is, or has been, an entrusted person; and

(b) the person has obtained a record in the person's capacity as an entrusted person; and

(c) the record:

(i) was acquired or prepared by or on behalf of the Organisation in connection with its functions; or

(ii) relates to the performance by the Organisation of its functions; and

(d) the person engages in any of the following conduct (the ***relevant conduct***):

(i) copying the record;

(ii) transcribing the record;

(iii) retaining the record;

(iv) removing the record;

(v) dealing with the record in any other manner; and

(e) the relevant conduct was not engaged in by the person:

(i) as an ASIO employee in the course of the person's duties as an ASIO employee; or

(ii) as an ASIO affiliate in accordance with the contract, agreement or other arrangement under which the person is performing functions or services for the Organisation; or

(iii) in accordance with a contract, agreement or arrangement the person has entered into with ASIO (other than as an ASIO affiliate); or

(iv) acting within the limits of authority conferred on the person by the Director-General; or

(v) with the approval of the Director-General, or of a person having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—record lawfully available

(2) Subsection (1) does not apply to a record that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person deals with the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the *Criminal Code*).

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 18B(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

Definitions

(5) In this section:

entrusted person means:

(a) an ASIO employee; or

(b) an ASIO affiliate; or

(c) a person who has entered into a contract, agreement or arrangement with ASIO (otherwise than as an ASIO affiliate).

record means a document, or any other object by which words, images, sounds or signals are recorded or stored or from which information can be obtained, and includes part of a record.

Note: For the definition of ***document***, see section 2B of the *Acts Interpretation Act 1901*.

signals includes electromagnetic emissions.

18B Unauthorised recording of information or matter

(1) A person commits an offence if:

(a) the person is, or has been, an entrusted person; and

(b) information or matter has come to the knowledge or into the possession of the person in the person's capacity as an entrusted person; and

(c) the information or matter:

(i) was acquired or prepared by or on behalf of the Organisation in connection with its functions; or

(ii) relates to the performance by the Organisation of its functions; and

(d) the person makes a record of the information or matter; and

(e) the record is not made by the person:

(i) as an ASIO employee in the course of the person's duties as an ASIO employee; or

(ii) as an ASIO affiliate in accordance with the contract, agreement or other arrangement under which the person is performing functions or services for the Organisation; or

(iii) in accordance with a contract, agreement or arrangement the person has entered into with ASIO (other than as an ASIO affiliate); or

(iv) acting within the limits of authority conferred on the person by the Director-General; or

(v) with the approval of the Director-General, or of a person having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person makes the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the *Criminal Code*).

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 18A(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

Definitions

(5) In this section:

entrusted person has the same meaning as in section 18A.

record has the same meaning as in section 18A.

18C Offences against section 18, 18A or 18B—general rules

Extended geographical jurisdiction

(1) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to an offence against section 18, 18A or 18B.

(2) Subsection (1) does not, by implication, affect the interpretation of any other provision of this Act.

Institution of prosecution

(3) A prosecution under section 18, 18A or 18B may be instituted only by, or with the consent of, the Attorney-General or a person acting under the Attorney-General's direction.

(4) However:

(a) a person charged with an offence against section 18, 18A or 18B may be arrested, or a warrant for his or her arrest may be issued and executed; and

(b) such a person may be remanded in custody or on bail;

even if the consent of the Attorney-General or a person acting under his or her direction has not been obtained, but no further proceedings are to be taken until that consent has been obtained.

(5) Nothing in subsection (3) or (4) prevents the discharging of the accused if proceedings are not continued within a reasonable time.

18D Offences against section 18, 18A or 18B—IGIS officials

(1) A person does not commit an offence against subsection 18(2), 18A(1) or 18B(1) if:

(a) the person is an IGIS official; and

(b) the relevant conduct is engaged in by the person for the purposes of exercising powers, or performing functions or duties, as an IGIS official.

(2) In a prosecution for an offence against subsection 18(2), 18A(1) or 18B(1), the defendant does not bear an evidential burden in relation to the matter in subsection (1) of this section, despite subsection 13.3(3) of the *Criminal Code*.

5 Section 22 (definition of *signals*)

Omit "light emissions and".

5A Subsections 92(1) and (1A) (penalty)

Repeal the penalty, substitute:

Penalty: Imprisonment for 10 years.

Intelligence Services Act 2001

6 Section 3

Insert:

IGIS official (short for Inspector-General of Intelligence and Security official) means:

(a) the Inspector-General of Intelligence and Security; or

(b) a member of the staff referred to in subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*.

record means a document, or any other object by which words, images, sounds or signals are recorded or stored or from which information can be obtained, and includes part of a record.

Note: For the definition of ***document***, see section 2B of the *Acts Interpretation Act 1901*.

7 Section 3

Insert:

signals includes electromagnetic emissions.

8 Before section 39

Insert:

Division 1—Secrecy

9 Paragraph 39(1)(a)

Before "prepared by", insert "acquired or".

10 Subsection 39(1) (penalty)

Repeal the penalty, substitute:

Penalty: Imprisonment for 10 years.

11 Subsection 39(2)

Repeal the subsection, substitute:

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(3) Subsection (1) does not apply if the person communicates the information or matter to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3): see subsection 13.3(3) of the *Criminal Code*).

12 Paragraph 39A(1)(a)

Before "prepared by", insert "acquired or".

13 Subsection 39A(1) (penalty)

Repeal the penalty, substitute:

Penalty: Imprisonment for 10 years.

14 Subsection 39A(2)

Repeal the subsection, substitute:

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(3) Subsection (1) does not apply if the person communicates the information or matter to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3): see subsection 13.3(3) of the *Criminal Code*.

15 Paragraph 40(1)(a)

Before "prepared by", insert "acquired or".

16 Subsection 40(1) (penalty)

Repeal the penalty, substitute:

Penalty: Imprisonment for 10 years.

17 Subsection 40(2)

Repeal the subsection, substitute:

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(3) Subsection (1) does not apply if the person communicates the information or matter to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3): see subsection 13.3(3) of the *Criminal Code*.

18 After section 40

Insert:

40A Communication of certain information—ONA

(1) A person commits an offence if:

(a) the person communicates any information or matter that was acquired or prepared by or on behalf of ONA in connection with its functions or relates to the performance by ONA of its functions; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of ONA; or

(ii) his or her having entered into any contract, agreement or arrangement with ONA; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ONA; and

(c) the communication was not made:

(i) to the Director-General of ONA or a staff member by the person in the course of the person's duties as a staff member; or

(ii) to the Director-General of ONA or a staff member by the person in accordance with a contract, agreement or arrangement; or

(iii) by the person in the course of the person's duties as a staff member, within the limits of authority conferred on the person by the Director-General of ONA; or

(iv) with the approval of the Director-General of ONA or of a staff member having the authority of the Director-General of ONA to give such an approval.

Penalty: Imprisonment for 10 years.

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(3) Subsection (1) does not apply if the person communicates the information or matter to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3): see subsection 13.3(3) of the *Criminal Code*).

40B Communication of certain information—DIO

(1) A person commits an offence if:

(a) the person communicates any information or matter that was acquired or prepared by or on behalf of DIO in connection with its functions or relates to the performance by DIO of its functions; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of DIO; or

(ii) his or her having entered into any contract, agreement or arrangement with DIO; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with DIO; and

(c) the communication was not made:

(i) to the Director of DIO or a staff member by the person in the course of the person's duties as a staff member; or

(ii) to the Director of DIO or a staff member by the person in accordance with a contract, agreement or arrangement; or

(iii) by the person in the course of the person's duties as a staff member, within the limits of authority conferred on the person by the Director of DIO; or

(iv) with the approval of the Director of DIO or of a staff member having the authority of the Director of DIO to give such an approval.

Penalty: Imprisonment for 10 years.

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(3) Subsection (1) does not apply if the person communicates the information or matter to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3): see subsection 13.3(3) of the *Criminal Code*.

40C Unauthorised dealing with records—ASIS

(1) A person commits an offence if:

(a) the person engages in any of the following conduct (the ***relevant conduct***):

(i) copying a record;

(ii) transcribing a record;

(iii) retaining a record;

(iv) removing a record;

(v) dealing with a record in any other manner; and

(b) the record was obtained by the person by reason of:

(i) his or her being, or having been, a staff member or agent of ASIS; or

(ii) his or her having entered into any contract, agreement or arrangement with ASIS; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIS; and

(c) the record:

(i) was acquired or prepared by or on behalf of ASIS in connection with its functions; or

(ii) relates to the performance by ASIS of its functions; and

(d) the relevant conduct was not engaged in:

(i) in the course of the person's duties as a staff member or agent; or

(ii) in accordance with a contract, agreement or arrangement with ASIS; or

(iii) by the person acting within the limits of authority conferred on the person by the Director-General; or

(iv) with the approval of the Director-General or of a staff member having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—record lawfully available

(2) Subsection (1) does not apply to a record that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person deals with the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:
  (a) is not satisfied that the defendant is guilty of the prosecuted offence; but
  (b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40D(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

40D Unauthorised recording of information or matter—ASIS

(1) A person commits an offence if:
  (a) the person makes a record of any information or matter; and
  (b) the information or matter has come to the knowledge or into the possession of the person by reason of:
    (i) his or her being, or having been, a staff member or agent of ASIS; or
    (ii) his or her having entered into any contract, agreement or arrangement with ASIS; or
    (iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIS; and
  (c) the information or matter:
    (i) was acquired or prepared by or on behalf of ASIS in connection with its functions; or
    (ii) relates to the performance by ASIS of its functions; and
  (d) the record was not made:
    (i) in the course of the person's duties as a staff member or agent; or
    (ii) in accordance with a contract, agreement or arrangement with ASIS; or
    (iii) by the person acting within the limits of authority conferred on the person by the Director-General; or

(iv) with the approval of the Director-General or of a staff member having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person makes the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40C(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

40E Unauthorised dealing with records—AGO

(1) A person commits an offence if:

(a) the person engages in any of the following conduct (the ***relevant conduct***):
  (i) copying a record;
  (ii) transcribing a record;
  (iii) retaining a record;
  (iv) removing a record;
  (v) dealing with a record in any other manner; and
(b) the record was obtained by the person by reason of:
  (i) his or her being, or having been, a staff member of AGO; or
  (ii) his or her having entered into any contract, agreement or arrangement with AGO; or
  (iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with AGO; and
(c) the record:
  (i) was acquired or prepared by or on behalf of AGO in connection with its functions; or
  (ii) relates to the performance by AGO of its functions; and
(d) the relevant conduct was not engaged in:
  (i) in the course of the person's duties as a staff member; or
  (ii) by the person in accordance with a contract, agreement or arrangement with AGO; or
  (iii) by the person acting within the limits of authority conferred on the person by the Director of AGO; or
  (iv) with the approval of the Director of AGO or of a staff member having the authority of the Director of AGO to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—record lawfully available

(2) Subsection (1) does not apply to a record that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person deals with the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40F(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

40F Unauthorised recording of information or matter—AGO

(1) A person commits an offence if:

(a) the person makes a record of any information or matter; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of AGO; or

(ii) his or her having entered into any contract, agreement or arrangement with AGO; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with AGO; and

(c) the information or matter:

(i) was acquired or prepared by or on behalf of AGO in connection with its functions; or

(ii) relates to the performance by AGO of its functions; and

(d) the record was not made:

(i) in the course of the person's duties as a staff member; or

(ii) in accordance with a contract, agreement or arrangement with AGO; or

(iii) by the person acting within the limits of authority conferred on the person by the Director of AGO; or

(iv) with the approval of the Director of AGO or of a staff member having the authority of the Director of AGO to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person makes the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40E(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the

defendant has been accorded procedural fairness in relation to that finding of guilt.

40G Unauthorised dealing with records—ASD

(1) A person commits an offence if:

(a) the person engages in any of the following conduct (the ***relevant conduct***):

(i) copying a record;

(ii) transcribing a record;

(iii) retaining a record;

(iv) removing a record;

(v) dealing with a record in any other manner; and

(b) the record was obtained by the person by reason of:

(i) his or her being, or having been, a staff member of ASD; or

(ii) his or her having entered into any contract, agreement or arrangement with ASD; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASD; and

(c) the record:

(i) was acquired or prepared by or on behalf of ASD in connection with its functions; or

(ii) relates to the performance by ASD of its functions; and

(d) the relevant conduct was not engaged in:

(i) in the course of the person's duties as a staff member; or

(ii) in accordance with a contract, agreement or arrangement with ASD; or

(iii) by the person acting within the limits of authority conferred on the person by the Director of ASD; or

(iv) with the approval of the Director of ASD or of a staff member having the authority of the Director of ASD to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—record lawfully available

(2) Subsection (1) does not apply to a record that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person deals with the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40H(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

40H Unauthorised recording of information or matter—ASD

(1) A person commits an offence if:

(a) the person makes a record of any information or matter; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of ASD; or

(ii) his or her having entered into any contract, agreement or arrangement with ASD; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASD; and

(c) the information or matter:

(i) was acquired or prepared by or on behalf of ASD in connection with its functions; or

(ii) relates to the performance by ASD of its functions; and

(d) the record was not made:

(i) in the course of the person's duties as a staff member; or

(ii) in accordance with a contract, agreement or arrangement with ASD; or

(iii) by the person acting within the limits of authority conferred on the person by the Director of ASD; or

(iv) with the approval of the Director of ASD or of a staff member having the authority of the Director of ASD to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person makes the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40G(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

40J Unauthorised dealing with records—ONA

(1) A person commits an offence if:

(a) the person engages in any of the following conduct (the ***relevant conduct***):

(i) copying a record;

(ii) transcribing a record;

(iii) retaining a record;

(iv) removing a record;

(v) dealing with a record in any other manner; and

(b) the record was obtained by the person by reason of:

(i) his or her being, or having been, a staff member of ONA; or

(ii) his or her having entered into any contract, agreement or arrangement with ONA; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ONA; and

(c) the record:

(i) was acquired or prepared by or on behalf of ONA in connection with its functions; or

(ii) relates to the performance by ONA of its functions; and

(d) the relevant conduct was not engaged in:

(i) in the course of the person's duties as a staff member; or

(ii) in accordance with a contract, agreement or arrangement with ONA; or

(iii) by the person acting within the limits of authority conferred on the person by the Director-General of ONA; or

(iv) with the approval of the Director-General of ONA or of a staff member having the authority of the Director-General of ONA to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—record lawfully available

(2) Subsection (1) does not apply to a record that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person deals with the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40K(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

40K Unauthorised recording of information or matter—ONA

(1) A person commits an offence if:

(a) the person makes a record of any information or matter; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of ONA; or

(ii) his or her having entered into any contract, agreement or arrangement with ONA; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ONA; and

(c) the information or matter:

(i) was acquired or prepared by or on behalf of ONA in connection with its functions; or

(ii) relates to the performance by ONA of its functions; and

(d) the record was not made:

(i) in the course of the person's duties as a staff member; or

(ii) in accordance with a contract, agreement or arrangement with ONA; or

(iii) by the person acting within the limits of authority conferred on the person by the Director-General of ONA; or

(iv) with the approval of the Director-General of ONA or of a staff member having the authority of the Director-General of ONA to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person makes the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40J(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

40L Unauthorised dealing with records—DIO

(1) A person commits an offence if:

(a) the person engages in any of the following conduct (the ***relevant conduct***):

(i) copying a record;

(ii) transcribing a record;

(iii) retaining a record;

(iv) removing a record;

(v) dealing with a record in any other manner; and

(b) the record was obtained by the person by reason of:

(i) his or her being, or having been, a staff member of DIO; or

(ii) his or her having entered into any contract, agreement or arrangement with DIO; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with DIO; and

(c) the record:

(i) was acquired or prepared by or on behalf of DIO in connection with its functions; or

(ii) relates to the performance by DIO of its functions; and

(d) the relevant conduct was not engaged in:

(i) in the course of the person's duties as a staff member; or

(ii) in accordance with a contract, agreement or arrangement with DIO; or

(iii) by the person acting within the limits of authority conferred on the person by the Director of DIO; or

(iv) with the approval of the Director of DIO or of a staff member having the authority of the Director of DIO to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—record lawfully available

(2) Subsection (1) does not apply to a record that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person deals with the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40M(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

40M Unauthorised recording of information or matter—DIO

(1) A person commits an offence if:

(a) the person makes a record of any information or matter; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of DIO; or

(ii) his or her having entered into any contract, agreement or arrangement with DIO; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with DIO; and

(c) the information or matter:

(i) was acquired or prepared by or on behalf of DIO in connection with its functions; or

(ii) relates to the performance by DIO of its functions; and

(d) the record was not made:

(i) in the course of the person's duties as a staff member; or

(ii) in accordance with a contract, agreement or arrangement with DIO; or

(iii) by the person acting within the limits of authority conferred on the person by the Director of DIO; or

(iv) with the approval of the Director of DIO or of a staff member having the authority of the Director of DIO to give such an approval.

Penalty: Imprisonment for 3 years.

Exception—information or matter lawfully available

(2) Subsection (1) does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

Exception—communication to the Inspector-General of Intelligence and Security

(2A) Subsection (1) does not apply if the person makes the record for the purpose of the Inspector-General of Intelligence and Security exercising a power, or performing a function or duty, under the *Inspector-General of Intelligence and Security Act 1986*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A): see subsection 13.3(3) of the *Criminal Code*.

Alternative verdict

(3) Subsection (4) applies if, in a prosecution for an offence (the ***prosecuted offence***) against subsection (1), the trier of fact:

(a) is not satisfied that the defendant is guilty of the prosecuted offence; but

(b) is satisfied beyond reasonable doubt that the defendant is guilty of an offence against subsection 40L(1) (the ***alternative offence***).

(4) The trier of fact may find the defendant not guilty of the prosecuted offence but guilty of the alternative offence, so long as the defendant has been accorded procedural fairness in relation to that finding of guilt.

19 Subsection 41(1)

Omit "(1)".

19A Subsection 41(1) (penalty)

Repeal the penalty, substitute:

Penalty: Imprisonment for 10 years.

20 Subsection 41(2)

Repeal the subsection.

21 After section 41

Insert:

41A Offences against this Division—general rules

Extended geographical jurisdiction

(1) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to an offence against this Division.

(2) Subsection (1) does not, by implication, affect the interpretation of any other provision of this Act.

Institution of prosecution

(3) A prosecution under this Division may be instituted only by, or with the consent of, the Attorney-General or a person acting under the Attorney-General's direction.

(4) However:

(a) a person charged with an offence against this Division may be arrested, or a warrant for his or her arrest may be issued and executed; and

(b) such a person may be remanded in custody or on bail;

even if the consent of the Attorney-General or a person acting under his or her direction has not been obtained, but no further proceedings are to be taken until that consent has been obtained.

(5) Nothing in subsection (3) or (4) prevents the discharging of the accused if proceedings are not continued within a reasonable time.

41B Offences against this Division—IGIS officials

(1) A person does not commit an offence against an information offence provision if:

(a) the person is an IGIS official; and

(b) the relevant conduct is engaged in by the person for the purpose of exercising powers, or performing functions or duties, as an IGIS official.

(2) In a prosecution for an offence against an information offence provision, the defendant does not bear an evidential burden in relation to the matter in subsection (1), despite subsection 13.3(3) of the *Criminal Code*.

(3) In this section:

information offence provision means subsection 39(1), 39A(1), 40(1), 40A(1), 40B(1), 40C(1), 40D(1), 40E(1), 40F(1), 40G(1), 40H(1), 40J(1), 40K(1), 40L(1) or 40M(1).

22 Before section 42

Insert:

Division 2—Other matters

23 Application of amendments

The amendments made by this Part apply in relation to conduct engaged in by a person in relation to records, information or matter after the commencement of this Part, whether the records were obtained, or the information or matter came to the knowledge or into the possession of the person, before or after that commencement.

Part 2—Consequential amendments

Australian Crime Commission Act 2002

24 Schedule 1

After "sections 18," insert "18A, 18B,".

Crimes Act 1914

25 Subsection 15LC(4) (note 2)

Omit "section 39 or 41", substitute "under Division 1 of Part 6".

Privacy Act 1988

26 Subsection 80P(7) (paragraph (a) of the definition of *designated secrecy provision*)

After "sections 18", insert ", 18A, 18B".

27 Subsection 80P(7) (paragraph (c) of the definition of *designated secrecy provision*)

Repeal the paragraph, substitute:

(c) sections 39, 39A, 40, 40A to 40M and 41 of the *Intelligence Services Act 2001*;

Schedule 7—Renaming of Defence agencies

Part 1—Main amendments

Intelligence Services Act 2001

1 Section 3 (definition of *agency*)

Omit "DIGO or DSD", substitute "AGO or ASD".

2 Section 3 (paragraphs (aa) and (b) of the definition of *agency head*)

Repeal the paragraphs, substitute:

(b) in relation to AGO—the Director of AGO; and

(c) in relation to ASD—the Director of ASD.

3 Section 3

Insert:

AGO means that part of the Defence Department known as the Australian Geospatial-Intelligence Organisation.

ASD means that part of the Defence Department known as the Australian Signals Directorate.

4 Section 3 (definition of *DIGO*)

Repeal the definition.

5 Section 3 (definition of *DSD*)

Repeal the definition.

6 Section 3 (paragraph (a) of the definition of *incidentally obtained intelligence*)

Omit "DIGO", substitute "AGO".

7 Section 3 (paragraph (a) of the definition of *incidentally obtained intelligence*)

Omit "DSD", substitute "ASD".

8 Section 3 (paragraph (b) of the definition of *intelligence information*)

Omit "DIGO", substitute "AGO".

9 Section 3 (paragraph (c) of the definition of *intelligence information*)

Omit "DSD", substitute "ASD".

10 Section 6B (heading)

Repeal the heading, substitute:

6B Functions of AGO

11 Section 6B

Omit "DIGO", substitute "AGO".

12 Section 7 (heading)

Repeal the heading, substitute:

7 Functions of ASD

13 Section 7

Omit "DSD", substitute "ASD".

14 Subsection 8(1)

Omit "DIGO", substitute "AGO".

15 Subsection 8(1)

Omit "DSD", substitute "ASD".

16 Paragraph 11(2)(e)

Omit "DIGO", substitute "AGO".

17 Paragraph 11(2)(f)

Omit "DSD", substitute "ASD".

18 Section 12A

Omit "Director of DIGO, the Director of DSD", substitute "Director of AGO, the Director of ASD".

19 Subsection 14(3) (definition of *staff member*)

Omit "Director of DIGO, the Director of DSD", substitute "Director of AGO, the Director of ASD".

20 Subsection 15(1)

Omit "responsible Minister in relation to DIGO and the responsible Minister in relation to DSD", substitute "responsible Minister in relation to AGO and the responsible Minister in relation to ASD".

21 Paragraph 15(3)(ab)

Omit "DIGO" (wherever occurring), substitute "AGO".

22 Paragraph 15(3)(b)

Omit "DSD" (wherever occurring), substitute "ASD".

23 Paragraph 29(1)(a)

Omit "DIGO" (first occurring), substitute "AGO".

24 Paragraph 29(1)(a)

Omit "DSD" (first occurring), substitute "ASD".

25 Paragraph 29(1)(a)

Omit "DIGO" (second occurring), substitute "AGO".

26 Paragraph 29(1)(a)

Omit "DSD" (second occurring), substitute "ASD".

27 Paragraph 29(1)(b)

Omit "DIGO", substitute "AGO".

28 Paragraph 29(1)(b)

Omit "DSD", substitute "ASD".

29 Subsection 29(2)

Omit "DIGO", substitute "AGO".

30 Subsection 29(2)

Omit "DSD", substitute "ASD".

31 Paragraph 29(3)(a)

Omit "DIGO", substitute "AGO".

32 Paragraph 29(3)(a)

Omit "DSD", substitute "ASD".

33 Paragraph 29(3)(b)

Omit "DIGO", substitute "AGO".

34 Paragraph 29(3)(b)

Omit "DSD", substitute "ASD".

35 Paragraph 29(3)(c)

Omit "DIGO", substitute "AGO".

36 Paragraph 29(3)(c)

Omit "DSD", substitute "ASD".

37 Paragraph 29(3)(e)

Omit "DIGO", substitute "AGO".

38 Paragraph 29(3)(e)

Omit "DSD", substitute "ASD".

39 Paragraph 29(3)(g)

Omit "DIGO", substitute "AGO".

40 Paragraph 29(3)(g)

Omit "DSD", substitute "ASD".

41 Paragraph 30(baa)

Omit "DIGO", substitute "AGO".

42 Paragraph 30(ba)

Omit "DSD", substitute "ASD".

43 Section 39A (heading)

Repeal the heading, substitute:

39A Communication of certain information—AGO

44 Subsection 39A(1)

Omit "DIGO" (wherever occurring), substitute "AGO".

45 Section 40 (heading)

Repeal the heading, substitute:

40 Communication of certain information—ASD

46 Subsection 40(1)

Omit "DSD" (wherever occurring), substitute "ASD".

47 Clause 1A of Schedule 1 (definition of *agency*)

Omit "DIGO", substitute "AGO".

48 Clause 1A of Schedule 1 (definition of *agency*)

Omit "DSD", substitute "ASD".

49 Clause 1A of Schedule 1 (paragraph (ba) of the definition of *agency head*)

Omit "DIGO", substitute "AGO".

50 Clause 1A of Schedule 1 (paragraph (c) of the definition of *agency head*)

Omit "DSD", substitute "ASD".

51 Clause 1A of Schedule 1 (paragraph (a) of the definition of *operationally sensitive information*)

Omit "DIGO", substitute "AGO".

52 Clause 1A of Schedule 1 (paragraph (a) of the definition of *operationally sensitive information*)

Omit "DSD", substitute "ASD".

53 Clause 1A of Schedule 1 (paragraph (b) of the definition of *operationally sensitive information*)

Omit "DIGO", substitute "AGO".

54 Clause 1A of Schedule 1 (paragraph (b) of the definition of *operationally sensitive information*)

Omit "DSD", substitute "ASD".

55 Paragraph 7(1)(a) of Schedule 1

Omit "DIGO or DSD", substitute "AGO or ASD".

56 Paragraph 20(2)(c) of Schedule 1

Omit "DIGO", substitute "AGO".

57 Paragraph 20(2)(c) of Schedule 1

Omit "DSD", substitute "ASD".

Part 2—Consequential amendments

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

58 Section 5

Insert:

> ***AGO*** means that part of the Defence Department known as the Australian Geospatial-Intelligence Organisation, and includes any part of the Defence Force that performs functions on behalf of that part of the Department.
>
> ***ASD*** means that part of the Defence Department known as the Australian Signals Directorate, and includes any part of the Defence Force that performs functions on behalf of that part of the Department.

59 Section 5 (definition of *defence intelligence agency*)

Omit "DIGO", substitute "AGO".

60 Section 5 (definition of *defence intelligence agency*)

Omit "DSD", substitute "ASD".

61 Section 5 (paragraph (gb) of the definition of *designated agency*)

Repeal the paragraph, substitute:

(gb) AGO; or

62 Section 5 (paragraph (gd) of the definition of *designated agency*)

Repeal the paragraph, substitute:

(gd) ASD; or

63 Section 5 (definition of *DIGO*)

Repeal the definition.

64 Section 5 (definition of *DIO*)

Omit "Department of Defence", substitute "Defence Department".

65 Section 5 (definition of *DSD*)

Repeal the definition.

66 Paragraph 128(13B)(d)

Omit "DIGO or DSD" (wherever occurring), substitute "AGO or ASD".

Archives Act 1983

67 Paragraphs 29(8)(ba) and (c)

Repeal the paragraphs, substitute:

(ba) the Australian Geospatial-Intelligence Organisation;

(c) the Australian Signals Directorate;

Australian Human Rights Commission Act 1986

68 Subsection 11(4)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

69 Subsection 11(4)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

70 Subsection 21(3)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

71 Subsection 21(3)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

Australian Security Intelligence Organisation Act 1979

72 Section 4

Insert:

AGO has the meaning given by the *Intelligence Services Act 2001*.

ASD has the meaning given by the *Intelligence Services Act 2001*.

73 Section 4 (definition of *DIGO*)

Repeal the definition.

74 Section 4 (definition of *DSD*)

Repeal the definition.

75 Section 4 (paragraph (c) of the definition of *intelligence or security agency*)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

76 Section 4 (paragraph (e) of the definition of *intelligence or security agency*)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

77 Subsection 18(4A) (heading)

Repeal the heading, substitute:

Communicating information to ASIS, ASD and AGO

78 Subsection 18(4A)

Omit "DSD or DIGO", substitute "ASD or AGO".

79 Paragraph 18(4A)(b)

Omit "DSD or DIGO's", substitute "ASD or AGO's".

80 Paragraphs 19A(1)(b) and (c)

Repeal the paragraphs, substitute:

(b) ASD;

(c) AGO;

81 Subsection 19A(4) (note 1)

Omit "DSD and DIGO", substitute "ASD and AGO".

82 Subsection 35(1) (paragraph (d) of the definition of *agency head*)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

83 Subsection 35(1) (paragraph (f) of the definition of *agency head*)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

Crimes Act 1914

84 Paragraph 15KY(3)(b)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

85 Paragraph 15KY(3)(c)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

86 Section 85ZL (paragraph (d) of the definition of *intelligence or security agency*)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

87 Section 85ZL (paragraph (f) of the definition of *intelligence or security agency*)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

Crimes (Overseas) Act 1964

88 Section 3

Insert:

> ***AGO*** has the same meaning as in the *Intelligence Services Act 2001*.
>
> ***ASD*** has the same meaning as in the *Intelligence Services Act 2001*.

89 Section 3 (definition of *DIGO*)

Repeal the definition.

90 Section 3 (definition of *DSD*)

Repeal the definition.

91 Section 3 (definition of *staff member*)

Omit "DIGO or DSD", substitute "AGO or ASD".

92 Subsection 3A(10) (heading)

Repeal the heading, substitute:

> *Defence Force members and ASIS, AGO and ASD staff not covered*

93 Paragraph 3A(10)(b)

Omit "DIGO or DSD" (wherever occurring), substitute "AGO or ASD".

94 Subsection 3A(10) (paragraph (a) of the note)

Omit "DIGO or DSD", substitute "AGO or ASD".

Criminal Code Act 1995

95 Section 473.1 of the *Criminal Code* (paragraph (d) of the definition of *intelligence or security officer*)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

96 Section 473.1 of the *Criminal Code* (definition of *intelligence or security officer*)

Omit "or the Defence Signals Directorate", substitute "or the Australian Signals Directorate".

97 Subsection 476.5(1) of the *Criminal Code*

Omit "DIGO or DSD", substitute "AGO or ASD".

98 Subsection 476.5(3) of the *Criminal Code*

Insert:

> ***AGO*** means that part of the Defence Department known as the Australian Geospatial-Intelligence Organisation.
>
> ***ASD*** means that part of the Defence Department known as the Australian Signals Directorate.

99 Subsection 476.5(3) of the *Criminal Code* (definition of *DIGO*)

Repeal the definition.

100 Subsection 476.5(3) of the *Criminal Code* (definition of *DSD*)

Repeal the definition.

101 Subsection 476.5(3) of the *Criminal Code* (paragraph (b) of the definition of *staff member*)

Omit "DSD" (wherever occurring), substitute "ASD".

102 Subsection 476.5(3) of the *Criminal Code* (paragraph (c) of the definition of *staff member*)

Omit "DIGO" (wherever occurring), substitute "AGO".

Freedom of Information Act 1982

103 Subsection 4(1)

Insert:

Australian Geospatial-Intelligence Organisation means that part of the Department of Defence known as the Australian Geospatial-Intelligence Organisation.

Australian Signals Directorate means that part of the Department of Defence known as the Australian Signals Directorate.

104 Subsection 4(1) (definition of *Defence Imagery and Geospatial Organisation*)

Repeal the definition.

105 Subsection 4(1) (definition of *Defence Signals Directorate*)

Repeal the definition.

106 Subparagraph 7(2A)(a)(v)

Repeal the subparagraph, substitute:

(v) the Australian Geospatial-Intelligence Organisation;

107 Subparagraph 7(2A)(a)(vii)

Repeal the subparagraph, substitute:

(vii) the Australian Signals Directorate;

108 Division 2 of Part I of Schedule 2

Insert:

Australian Geospatial-Intelligence Organisation

Australian Signals Directorate

109 Division 2 of Part I of Schedule 2

Omit:

Defence Imagery and Geospatial Organisation

110 Division 2 of Part I of Schedule 2

Omit:

Defence Signals Directorate

Independent National Security Legislation Monitor Act 2010

111 Section 4 (paragraph (f) of the definition of *head*)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

112 Section 4 (paragraph (h) of the definition of *head*)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

113 Section 4 (paragraph (g) of the definition of *law enforcement or security agency*)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

114 Section 4 (paragraph (i) of the definition of *law enforcement or security agency*)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

Inspector-General of Intelligence and Security Act 1986

115 Subsection 3(1)

Insert:

> ***AGO*** means that part of the Defence Department known as the Australian Geospatial-Intelligence Organisation, and any part of the Defence Force that performs functions on behalf of that part of the Department.
>
> ***ASD*** means that part of the Defence Department known as the Australian Signals Directorate, and includes any part of the Defence Force that performs functions on behalf of that part of that Department.

116 Subsection 3(1) (definition of *DIGO*)

Repeal the definition.

117 Subsection 3(1) (definition of *DSD*)

Repeal the definition.

118 Subsection 3(1) (paragraph (c) of the definition of *head*)

Repeal the paragraph, substitute:

(c) in relation to AGO—the Director of AGO; or

119 Subsection 3(1) (paragraph (e) of the definition of *head*)

Repeal the paragraph, substitute:

(e) in relation to ASD—the Director of ASD; or

120 Subsection 3(1) (definition of *intelligence agency*)

Omit "DIGO", substitute "AGO".

121 Subsection 3(1) (definition of *intelligence agency*)

Omit "DSD", substitute "ASD".

122 Subsections 8(2) and (4)

Omit "DIGO or DSD", substitute "AGO or ASD".

123 Subsection 8(5)

Omit "DIGO, DSD", substitute "AGO, ASD".

124 Paragraph 8A(4)(a)

Omit "DIGO or DSD", substitute "AGO or ASD".

125 Paragraph 15(3)(b)

Omit "DIGO", substitute "AGO".

126 Paragraph 15(3)(b)

Omit "DSD", substitute "ASD".

127 Paragraph 21(1B)(b)

Omit "DIGO", substitute "AGO".

128 Paragraph 21(1B)(b)

Omit "DSD", substitute "ASD".

129 Paragraph 32A(1)(d)

Omit "DIGO", substitute "AGO".

130 Paragraph 32A(1)(d)

Omit "DSD", substitute "ASD".

131 Paragraph 32A(5)(b)

Omit "DIGO", substitute "AGO".

132 Paragraph 32A(5)(b)

Omit "DSD", substitute "ASD".

133 Subsection 32B(1)

Omit "DIGO or DSD", substitute "AGO or ASD".

134 Subsection 35(2B)

Omit "and DSD", substitute ", AGO and ASD".

Privacy Act 1988

135 Paragraph 7(1)(g)

Omit "Defence Imagery and Geospatial Organisation or the Defence Signals Directorate", substitute "Australian Geospatial-Intelligence Organisation or the Australian Signals Directorate".

136 Paragraph 7(1A)(c)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

137 Paragraph 7(2)(b)

Omit "Defence Imagery and Geospatial Organisation or the Defence Signals Directorate", substitute "Australian Geospatial-Intelligence Organisation or the Australian Signals Directorate".

Public Interest Disclosure Act 2013

138 Section 8 (paragraph (c) of the definition of *intelligence agency*)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

139 Section 8 (paragraph (e) of the definition of *intelligence agency*)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

140 Paragraph 72(1)(g)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

141 Paragraph 72(1)(i)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

142 Paragraph 72(4)(a)

Omit "Defence Imagery and Geospatial Organisation", substitute "Australian Geospatial-Intelligence Organisation".

143 Paragraph 72(4)(c)

Omit "Defence Signals Directorate", substitute "Australian Signals Directorate".

Part 3—Transitional provisions

144 Transitional—subsection 25B(1) of the *Acts Interpretation Act 1901*

Subsection 25B(1) of the *Acts Interpretation Act 1901* applies as if:

(a) that part of the Defence Department known as the Defence Imagery and Geospatial Organisation were a body and the amendments made by Part 1 of this Schedule altered the name of that body to the Australian Geospatial-Intelligence Organisation; and

(b) that part of the Defence Department known as the Defence Signals Directorate were a body and the amendments made by Part 1 of this Schedule altered the name of that body to the Australian Signals Directorate.

145 Transitional rules

The Minister may, by legislative instrument, make rules in relation to transitional matters arising out of the amendments and repeals made by Parts 1 and 2 of this Schedule.

[*Minister's second reading speech made in—*
Senate on 16 July 2014
House of Representatives on 1 October 2014]

(178/14)