

2013-2014

The Parliament of the
Commonwealth of Australia

THE SENATE

Presented and read a first time

**National Security Legislation
Amendment Bill (No. 1) 2014**

No. , 2014

(Attorney-General)

**A Bill for an Act to amend the law relating to
national security and intelligence services, and for
related purposes**

Contents

1	Short title.....	1
2	Commencement.....	1
3	Schedule(s).....	2
Schedule 1—ASIO employment etc.		3
Part 1—Main amendments		3
<i>Australian Security Intelligence Organisation Act 1979</i>		3
Part 2—Other amendments		11
<i>Administrative Appeals Tribunal Act 1975</i>		11
<i>Australian Postal Corporation Act 1989</i>		11
<i>Crimes Act 1914</i>		12
<i>Criminal Code Act 1995</i>		12
<i>Inspector-General of Intelligence and Security Act 1986</i>		13
<i>Public Interest Disclosure Act 2013</i>		14
<i>Surveillance Devices Act 2004</i>		15
<i>Taxation Administration Act 1953</i>		15
<i>Telecommunications (Interception and Access) Act 1979</i>		16
Part 3—Transitional and application provisions		20
Schedule 2—Powers of the Organisation		24
Part 1—Amendments		24
<i>Australian Security Intelligence Organisation Act 1979</i>		24
Part 2—Consequential amendments		58
<i>Telecommunications (Interception and Access) Act 1979</i>		58
Part 3—Application, transitional and savings provisions		59
Schedule 3—Protection for special intelligence operations		60
<i>Australian Security Intelligence Organisation Act 1979</i>		60
Schedule 4—ASIO co-operation and information sharing		72
<i>Australian Security Intelligence Organisation Act 1979</i>		72

Schedule 5—Activities and functions of Intelligence Services Act 2001 agencies	73
Schedule 6—Protection of information	81
Part 1—Main amendments	81
<i>Australian Security Intelligence Organisation Act 1979</i>	81
<i>Intelligence Services Act 2001</i>	86
Part 2—Consequential amendments	106
<i>Australian Crime Commission Act 2002</i>	106
<i>Crimes Act 1914</i>	106
<i>Privacy Act 1988</i>	106
Schedule 7—Renaming of Defence agencies	107
Part 1—Main amendments	107
<i>Intelligence Services Act 2001</i>	107
Part 2—Consequential amendments	113
<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>	113
<i>Archives Act 1983</i>	114
<i>Australian Human Rights Commission Act 1986</i>	114
<i>Australian Security Intelligence Organisation Act 1979</i>	115
<i>Crimes Act 1914</i>	116
<i>Crimes (Overseas) Act 1964</i>	117
<i>Criminal Code Act 1995</i>	117
<i>Freedom of Information Act 1982</i>	118
<i>Independent National Security Legislation Monitor Act 2010</i>	120
<i>Inspector-General of Intelligence and Security Act 1986</i>	120
<i>Privacy Act 1988</i>	122
<i>Public Interest Disclosure Act 2013</i>	123
Part 3—Transitional provisions	124

1 **A Bill for an Act to amend the law relating to**
2 **national security and intelligence services, and for**
3 **related purposes**

4 The Parliament of Australia enacts:

5 **1 Short title**

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

8 **2 Commencement**

9 (1) Each provision of this Act specified in column 1 of the table
10 commences, or is taken to have commenced, in accordance with
11 column 2 of the table. Any other statement in column 2 has effect
12 according to its terms.
13

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. Schedules 1 to 6	The 28th day after this Act receives the Royal Assent.	
3. Schedule 7, items 1 to 110	The day after this Act receives the Royal Assent.	
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 <i>Independent National Security Legislation Monitor Repeal Act 2014</i> commences at or before that time, the provision(s) do not commence at all.	
5. Schedule 7, items 115 to 145	The day after this Act receives the Royal Assent.	

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

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

7 **3 Schedule(s)**

8 Each Act that is specified in a Schedule to this Act is amended or
9 repealed as set out in the applicable items in the Schedule
10 concerned, and any other item in a Schedule to this Act has effect
11 according to its terms.

1 **Schedule 1—ASIO employment etc.**

2 **Part 1—Main amendments**

3 *Australian Security Intelligence Organisation Act 1979*

4 **1 Section 4**

5 Insert:

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

11 *ASIO employee* means a person employed under section 84 or 90.

12 **2 Section 4 (definition of *Deputy Director-General*)**

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

15 **3 Section 4**

16 Insert:

17 *senior position-holder* means an ASIO employee, or an ASIO
18 affiliate, who holds, or is acting in, a position in the Organisation
19 that is:

- 20 (a) equivalent to or higher than a position occupied by an SES
21 employee; or
22 (b) known as Coordinator.

23 **4 Paragraph 8A(1)(b)**

24 Omit “sections 85 and 86”, substitute “sections 84, 85, 86 and 87”.

25 **5 Section 16**

26 Repeal the section, substitute:

1 **16 Delegation**

2 (1) The Director-General may, by signed writing, delegate to a person
3 any of the Director-General's powers, functions or duties under or
4 for the purposes of this Act that relate to:

- 5 (a) the management of ASIO employees or ASIO affiliates; or
6 (b) the financial management of the Organisation.

7 Note: For further provisions relating to delegations, see sections 34AB and
8 34A of the *Acts Interpretation Act 1901*.

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

12 **6 Subsection 18(2)**

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

14 *Offence for unauthorised communication of information or matter*

15 (2) A person commits an offence if:

- 16 (a) the person makes a communication of any information or
17 matter; and
18 (b) the information or matter has come to the knowledge or into
19 the possession of the person by reason of:
20 (i) his or her being, or having been, an ASIO employee; or
21 (ii) his or her being, or having been, an ASIO affiliate; or
22 (iii) his or her having entered into a contract, agreement or
23 arrangement with ASIO (otherwise than as an ASIO
24 affiliate); and
25 (c) the information or matter:
26 (i) was acquired or prepared by or on behalf of the
27 Organisation in connection with its functions; or
28 (ii) relates to the performance by the Organisation of its
29 functions; and
30 (d) the communication was not made to the Director-General, an
31 ASIO employee or an ASIO affiliate:
32 (i) by an ASIO employee, in the course of the ASIO
33 employee's duties; or
34 (ii) by an ASIO affiliate, in accordance with the contract,
35 agreement or other arrangement under which the ASIO
-

- 1 affiliate is performing functions or services for the
2 Organisation; or
3 (iii) by a person who has entered into a contract, agreement
4 or arrangement with ASIO (otherwise than as an ASIO
5 affiliate), in accordance with the contract, agreement or
6 arrangement; and
7 (e) the communication was not made by a person acting within
8 the limits of authority conferred on the person by the
9 Director-General; and
10 (f) the communication was not made with the approval of the
11 Director-General or of a person having the authority of the
12 Director-General to give such an approval.

13 **7 Subsection 19A(3)**

14 Omit “officers and employees, and other resources, of the
15 Organisation”, substitute “ASIO employees and ASIO affiliates, and
16 other resources of the Organisation”.

17 **8 Subsection 23(1)**

18 Omit “an authorised officer or employee”, substitute “the
19 Director-General or an authorised person”.

20 **9 Subsection 23(6)**

21 Repeal the subsection, substitute:

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

25 (6A) The Director-General may, in writing, appoint a senior-position
26 holder, or a class of senior position-holders, for the purposes of
27 subsection (6).

28 **10 Subsection 23(7) (definition of *authorised officer or***
29 ***employee*)**

30 Repeal the definition.

31 **11 Subsection 23(7)**

32 Insert:

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

3 **12 Subsection 23(7) (definition of *senior officer of the***
4 ***Organisation*)**

5 Repeal the definition.

6 **13 Subsection 25A(4) (note)**

7 Omit “an ASIO officer”, substitute “a person”.

8 **14 Subsection 25A(4) (note)**

9 Omit “the ASIO officer”, substitute “the person”.

10 **15 Subsections 27(1) and 27AA(1)**

11 Omit “an officer, employee or agent of the Organisation” (wherever
12 occurring), substitute “the Director-General, an ASIO employee or an
13 ASIO affiliate”.

14 **16 Paragraph 34ZC(2)(c)**

15 Repeal the paragraph, substitute:
16 (c) an ASIO employee or an ASIO affiliate;

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

18 Repeal the subparagraph, substitute:
19 (iii) an ASIO employee or an ASIO affiliate;

20 **18 Part V (heading)**

21 Repeal the heading, substitute:

22 **Part V—ASIO employees etc.**

23 **19 Sections 84 to 89**

24 Repeal the sections, substitute:

1 **84 Employees of the Organisation**

2 *Employees*

- 3 (1) The Director-General may, on behalf of the Commonwealth,
4 employ such persons as he or she considers necessary for the
5 performance of the Organisation's functions and the exercise of the
6 Organisation's powers.
- 7 (2) The Director-General may from time to time determine in writing
8 the terms and conditions of employment applying to persons
9 employed under subsection (1).
- 10 (3) The Director-General, on behalf of the Commonwealth, has all the
11 rights, duties and powers of an employer in respect of persons
12 employed under subsection (1).
- 13 (4) Without limiting subsection (3), the Director-General has, in
14 respect of persons employed under subsection (1), the rights, duties
15 and powers that are prescribed by regulation.

16 *Termination of employment*

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

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

22 **85 Consultants and contractors**

- 23 (1) The Director-General may engage persons as consultants or
24 contractors to the Organisation.
- 25 (2) An engagement under subsection (1) is to be made:
26 (a) on behalf of the Commonwealth; and
27 (b) by written agreement.

1 **86 Secondment of ASIO employees**

2 *Secondment*

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

6 *Termination of secondment*

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

10 **87 Secondment of persons to the Organisation**

- 11 (1) The Director-General may, by written agreement with a body or
12 organisation (whether within or outside Australia), arrange for a
13 person who is an officer, employee or other member of staff of the
14 body or organisation to be made available to the Organisation to
15 perform services in connection with the performance or the
16 exercise of any of the Organisation's functions or powers.
- 17 (2) The terms and conditions (including remuneration and allowances)
18 applicable to a person performing services under an agreement are
19 those specified in the agreement.

20 **88 Applicability of principles of the *Public Service Act 1999***

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

26 **89 Voluntary moves to APS**

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

- 1 (2) An ASIO employee who moves to an APS Agency under that
2 section is entitled to have his or her employment, as an ASIO
3 employee, treated as if it were:
4 (a) employment as an APS employee; and
5 (b) at a corresponding classification, as agreed between the
6 Director-General and the Australian Public Service
7 Commissioner.

8 **20 Section 90 (heading)**

9 Repeal the heading, substitute:

10 **90 Regulations relating to employment of persons**

11 **21 Subsection 90(1)**

12 Omit “officers otherwise than under agreements in writing and may, in
13 respect of officers”, substitute “persons otherwise than under section 84
14 and may, in respect of persons”.

15 **22 Subsection 90(2)**

16 Repeal the subsection.

17 **23 Subsection 90(2A)**

18 Omit “persons who are or have been officers or temporary or casual
19 employees”, substitute “persons who are ASIO employees, ASIO
20 affiliates, former ASIO employees or former ASIO affiliates”.

21 **24 Subsection 90(3)**

22 Omit “notwithstanding sections 84, 85 and 86”, substitute “despite
23 section 84”.

24 **25 Subsection 90(4)**

25 Repeal the subsection.

26 **26 Section 91**

27 Omit “officers and employees of the Organisation”, substitute “ASIO
28 employees and ASIO affiliates”.

29 **27 Section 92 (heading)**

30 Repeal the heading, substitute:

1 **92 Publication of identity of ASIO employee or ASIO affiliate**

2 **28 Subsection 92(1)**

3 Omit all the words after “residing at”, substitute:

4 a particular address, is:

- 5 (a) an ASIO employee or ASIO affiliate, or is in any way
6 connected with an ASIO employee or ASIO affiliate; or
7 (b) subject to subsection (1B), is a former ASIO employee or
8 former ASIO affiliate or is in any way connected with a
9 former ASIO employee or former ASIO affiliate.

10 **29 Subsection 92(1A)**

11 Omit all the words after “residing at”, substitute:

12 a particular address, is:

- 13 (a) an ASIO employee or ASIO affiliate, or is in any way
14 connected with an ASIO employee or ASIO affiliate; or
15 (b) subject to subsection (1B), is a former ASIO employee or
16 former ASIO affiliate, or is in any way connected with a
17 former ASIO employee or former ASIO affiliate.

18 **30 Subsection 92(1B)**

19 Omit “former officer, employee or agent of the Organisation” (wherever
20 occurring), substitute “former ASIO employee or former ASIO
21 affiliate”.

1 **Part 2—Other amendments**

2 *Administrative Appeals Tribunal Act 1975*

3 **31 Subsection 3(1)**

4 Insert:

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

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

9 **32 Subsections 19(3B), 21AA(3) and 21AB(3)**

10 Omit “an officer, employee or agent of the Australian Security
11 Intelligence Organisation”, substitute “an ASIO employee or ASIO
12 affiliate”.

13 **33 Subsection 39A(15)**

14 Repeal the subsection, substitute:

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

17 (a) an ASIO employee or ASIO affiliate; or

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

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

23 *Australian Postal Corporation Act 1989*

24 **34 Subsection 90F(1)**

25 Omit “an officer or employee of ASIO”, substitute “a person”.

26 **35 Paragraph 90F(2)(b)**

27 Omit “an officer or employee of ASIO”, substitute “a person”.

1 **36 Paragraph 90LD(2)(a)**

2 Repeal the paragraph, substitute:

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

7 ***Crimes Act 1914***

8 **37 Paragraph 15LH(3) (paragraph (f) of the definition of**
9 ***senior officer*)**

10 Omit “senior officer of the Australian Security Intelligence
11 Organisation as defined in section 24 of the *Australian Security*
12 *Intelligence Organisation Act 1979*, or a person occupying an
13 equivalent or higher position in the Australian Security Intelligence
14 Organisation”, substitute “senior position-holder within the meaning of
15 the *Australian Security Intelligence Organisation Act 1979*”.

16 ***Criminal Code Act 1995***

17 **38 Subsection 100.1(1) of the *Criminal Code***

18 Insert:

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

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

23 **39 Subparagraph 105.39(2)(b)(vi) of the *Criminal Code***

24 Omit “officer or employee of the Australian Security Intelligence
25 Organisation”, substitute “ASIO employee or an ASIO affiliate”.

26 **40 Subsections 105.42(2) and (3) of the *Criminal Code***

27 Omit “officer or employee of the Australian Security Intelligence
28 Organisation”, substitute “ASIO employee or an ASIO affiliate”.

1 **41 Subparagraph 105.43(11)(c)(iv) of the *Criminal Code***

2 Omit “officer or employee of the Australian Security Intelligence
3 Organisation”, substitute “ASIO employee or an ASIO affiliate”.

4 ***Inspector-General of Intelligence and Security Act 1986***

5 **42 Subsection 3(1)**

6 Insert:

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

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

11 **43 Paragraph 8(1)(b)**

12 Omit “employees of ASIO”, substitute “ASIO employees and ASIO
13 affiliates”.

14 **44 Paragraph 8(7)(a)**

15 Omit “Director-General of Security or ASIO employees”, substitute
16 “Director-General of Security, ASIO employees or ASIO affiliates”.

17 **45 After subsection 8(7)**

18 Insert:

- 19 (8) The functions of the Inspector-General include inquiring into a
20 matter to which a complaint to the Inspector-General made by an
21 ASIO affiliate relates to the extent that the matter is related to:
- 22 (a) the contract, agreement or other arrangement under which the
23 ASIO affiliate is performing functions or services for ASIO;
24 or
 - 25 (b) the performance of functions or services by the ASIO
26 affiliate under the contract, agreement or other arrangement.

- 27 (8A) However, the Inspector-General may decide not to inquire into a
28 matter referred to in subsection (8) if the Inspector-General is
29 satisfied that the ASIO affiliate can have the matter reviewed by a
30 body constituted by, or including, persons other than the
31 Director-General of Security, ASIO employees or ASIO affiliates.

1 **46 Paragraph 11(5)(a)**

2 Omit “employees of that agency”, substitute “ASIO employees or ASIS
3 employees (as the case may be)”.

4 **47 At the end of paragraph 11(5)(a)**

5 Add “or”.

6 **48 At the end of section 11**

7 Add:

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

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

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

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

19 ***Public Interest Disclosure Act 2013***

20 **49 Subparagraph 41(1)(f)(i)**

21 Omit “or the Australian Security Intelligence Organisation”.

22 **50 After paragraph 41(1)(f)**

23 Insert:

24 (fa) information:

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

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

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

3 **51 Subsection 41(3)**

4 Repeal the subsection, substitute:

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

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

11 **52 Section 66 (table item 7)**

12 Omit “agency to which the agent or member of the staff referred to in
13 that paragraph belongs”, substitute “Australian Secret Intelligence
14 Service”.

15 **53 Section 66 (after table item 7)**

16 Insert:

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

17 ***Surveillance Devices Act 2004***

18 **54 Subparagraph 45(4)(e)(i)**

19 Omit “officer or employee of the Australian Security Intelligence
20 Organisation”, substitute “ASIO employee (within the meaning of the
21 *Australian Security Intelligence Organisation Act 1979*) or an ASIO
22 affiliate (within the meaning of that Act)”.

23 ***Taxation Administration Act 1953***

24 **55 Paragraph 355-70(2)(b) in Schedule 1**

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

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

2 Omit “officers or employees of ASIO”, substitute “ASIO employees
3 (within the meaning of the *Australian Security Intelligence*
4 *Organisation Act 1979*) or ASIO affiliates (within the meaning of that
5 Act)”.

6 ***Telecommunications (Interception and Access) Act 1979***

7 **57 Subsection 5(1)**

8 Insert:

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

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

13 **58 Subsection 5(1) (definition of *Deputy Director-General of***
14 ***Security*)**

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

17 **59 Section 5AD**

18 Omit “senior officer of the Organisation (within the meaning of
19 section 24”, substitute “senior position-holder (within the meaning”.

20 **60 Paragraph 7(2)(ac)**

21 Omit “officer of the Organisation”, substitute “ASIO employee”.

22 **61 After paragraph 7(2)(ac)**

23 Insert:

- 24 (ad) the interception of a communication where the interception
25 results from, or is incidental to, action taken by an ASIO
26 affiliate, in accordance with the contract, agreement or other
27 arrangement under which the ASIO affiliate is performing
28 functions or services for the Organisation, for the purpose of:
29 (i) discovering whether a listening device is being used at,
30 or in relation to, a particular place; or
31 (ii) determining the location of a listening device; or
-

1 **62 Section 12**

2 Omit “an officer of the Organisation”, substitute “an ASIO employee or
3 ASIO affiliate”.

4 **63 Section 12**

5 Omit “officers and employees of the Organisation and other persons”,
6 substitute “any persons”.

7 **64 Subsection 18(4)**

8 Omit all the words after “respect”, substitute:

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

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

12 (b) in connection with:

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

14 (ii) the making use of; or

15 (iii) the making of a record of; or

16 (iv) the custody of a record of; or

17 (v) the giving in evidence of;

18 information obtained by the execution of such a warrant.

19 **65 Paragraph 55(3)(c)**

20 Repeal the paragraph, substitute:

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

22 **66 Subsection 55(8)**

23 Omit “officer or employee of the Organisation”, substitute “ASIO
24 employee”.

25 **67 Subsection 64(2)**

26 Omit “officer or employee of the Organisation”, substitute “ASIO
27 employee or ASIO affiliate”.

28 **68 Paragraph 108(2)(g)**

29 Omit “an officer of the Organisation”, substitute “an ASIO employee”.

1 **69 After paragraph 108(2)(g)**

2 Insert:

- 3 (ga) accessing a stored communication if the access results from,
4 or is incidental to, action taken by an ASIO affiliate, in
5 accordance with the contract, agreement or other
6 arrangement under which the ASIO affiliate is performing
7 functions or services for the Organisation, for the purpose of:
8 (i) discovering whether a listening device is being used at,
9 or in relation to, a particular place; or
10 (ii) determining the location of a listening device; or

11 **70 Subsections 136(2) and (3)**

12 Omit “officer or employee of the Organisation”, substitute “ASIO
13 employee or ASIO affiliate”.

14 **71 Subsection 136(3)**

15 Omit “such officer or employee”, substitute “ASIO employee or ASIO
16 affiliate”.

17 **72 Subsection 136(4)**

18 Omit “officer or employee of the Organisation”, substitute “ASIO
19 employee or ASIO affiliate”.

20 **73 Subsection 174(2)**

21 Omit “an officer or employee of the Organisation”, substitute “any
22 other ASIO employee or ASIO affiliate”.

23 **74 Section 175**

24 Omit “officer or employee of the Organisation” (wherever occurring),
25 substitute “ASIO employee or ASIO affiliate”.

26 **75 Paragraph 176(2)(c)**

27 Omit “officer or employee of the Organisation”, substitute “ASIO
28 employee or ASIO affiliate”.

29 **76 Subsections 184(1) and (2)**

30 Omit “officer or employee of the Organisation”, substitute “ASIO
31 employee or ASIO affiliate”.

- 1 **77 Paragraphs 185B(1)(a) and (b)**
2 Omit “officer or employee of the Organisation”, substitute “ASIO
3 employee or ASIO affiliate”.

1 **Part 3—Transitional and application provisions**

2 **78 Transitional—delegations**

- 3 (1) This item applies to a delegation if the delegation was in force under
4 section 16 of the *Australian Security Intelligence Organisation Act*
5 *1979* immediately before the commencement of this Schedule.
- 6 (2) The delegation has effect, after that commencement, as if the delegation
7 had been made under section 16 of that Act as amended by this
8 Schedule.

9 **79 Transitional—requesting information or documents from**
10 **operators of aircraft or vessels**

- 11 (1) If, immediately before the commencement of this Schedule, a person
12 was an authorised officer or employee within the meaning of section 23
13 of the *Australian Security Intelligence Organisation Act 1979*, the
14 person is taken, after that commencement, to be an authorised person
15 within the meaning of that section as amended by this Schedule.
- 16 (2) If, immediately before the commencement of this Schedule, a person
17 was an authorising officer for the purposes of subsection 23(6) of the
18 *Australian Security Intelligence Organisation Act 1979*, the person is
19 taken, after that commencement, to be a person appointed under
20 subsection 23(6A) of that Act as inserted by this Schedule.

21 **80 Application and transitional—employees of the**
22 **Organisation**

- 23 A person who, immediately before the commencement of this Schedule,
24 was an officer or employee of the Organisation employed under
25 section 84 of the *Australian Security Intelligence Organisation Act*
26 *1979*, is, immediately after that commencement, taken to be employed:
- 27 (a) under subsection 84(1) of that Act as in force immediately
28 after that commencement; and
- 29 (b) on the terms and conditions that were applicable to the
30 person immediately before that commencement.

1 **81 Employees of the Organisation—acquisition of property**

- 2 (1) This item applies to a person who, immediately before the
3 commencement of this Schedule, was an officer or employee of the
4 Organisation employed under section 84 of the *Australian Security*
5 *Intelligence Organisation Act 1979*.
- 6 (2) Section 84 of the *Australian Security Intelligence Organisation Act*
7 *1979*, as substituted by this Schedule, does not apply to the extent (if
8 any) to which the operation of that section would result in the
9 acquisition of property (within the meaning of paragraph 51(xxxi) of the
10 Constitution) from the person otherwise than on just terms (within the
11 meaning of that paragraph).

12 **82 Transitional—former officers, employees or agents**

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

19 **83 Transitional—authorisations under the *Australian Postal***
20 ***Corporation Act 1989***

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

26 **84 Transitional—delegations under the *Crimes Act 1914***

- 27 (1) This item applies to a delegation if the delegation was in force
28 immediately before the commencement of this Schedule under
29 section 15LH of the *Crimes Act 1914* in relation to a person referred to
30 in paragraph (f) of the definition of *senior officer* in
31 subsection 15LH(3) of that Act.
- 32 (2) The delegation has effect, after that commencement, as if the delegation
33 had been made under that section in relation to a person referred to in
34 that paragraph as amended by this Schedule.

1 **85 Transitional—determinations under the *Public Interest***
2 ***Disclosure Act 2013***

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

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

15 **86 Transitional—authorisations under the *Taxation***
16 ***Administration Act 1953***

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

23 **87 Transitional provisions—*Telecommunications***
24 ***(Interception and Access) Act 1979***

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

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

- 1 (3) If, immediately before the commencement of this Schedule, a person
2 was approved under section 12 of the *Telecommunications (Interception*
3 *and Access) Act 1979*, the person is taken, after that commencement, to
4 be a person approved under that section as amended by this Schedule.
- 5 (4) If, immediately before the commencement of this Schedule, a person
6 was approved under paragraph 55(3)(c) of the *Telecommunications*
7 *(Interception and Access) Act 1979* to exercise the authority conferred
8 by warrants (or classes of warrants), the person is taken, after that
9 commencement, to be approved under that paragraph as amended by
10 this Schedule.

1 **Schedule 2—Powers of the Organisation**

2 **Part 1—Amendments**

3 *Australian Security Intelligence Organisation Act 1979*

4 **1 Section 4 (definition of certified copy)**

5 Repeal the definition, substitute:

6 *certified copy* means:

- 7 (a) in relation to a warrant—a copy of the warrant that has been
8 certified in writing by the Director-General or a Deputy
9 Director-General to be a true copy of the warrant; or
10 (b) in relation to an authorisation under section 27G—a copy of
11 the authorisation that has been certified in writing by the
12 Director-General or a Deputy Director-General to be a true
13 copy of the authorisation; or
14 (c) in relation to an instrument varying or revoking a warrant or
15 an authorisation under section 27G—a copy of the instrument
16 that has been certified in writing by the Director-General or a
17 Deputy Director-General to be a true copy of the instrument.

18 **2 Before section 22**

19 Insert:

20 **Subdivision A—Preliminary**

21 **3 Section 22**

22 Insert:

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

26 **4 Section 22 (definition of computer)**

27 Repeal the definition, substitute:

28 *computer* means all or part of:

- 29 (a) one or more computers; or

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

4 **5 Section 22**

5 Insert:

6 *device* includes instrument, apparatus and equipment.

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

10 *identified person warrant* means a warrant issued under
11 section 27C.

12 *install* includes attach and apply.

13 **6 Section 22 (definition of *listening device*)**

14 Repeal the definition, substitute:

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

22 **7 Section 22**

23 Insert:

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

26 *object* means:

- 27 (a) a vehicle, aircraft, vessel or other means of transportation; or
28 (b) clothing or any other thing worn; or
29 (c) any other thing.

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

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

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

8 ***surveillance device*** means:

- 9 (a) a listening device, an optical surveillance device or a tracking
10 device; or
11 (b) a device that is a combination of any 2 or more of the devices
12 referred to in paragraph (a) or (c); or
13 (c) a device of a kind prescribed by regulation for the purposes
14 of this paragraph.

15 ***surveillance device warrant*** means a warrant issued under
16 section 26.

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

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

22 ***use*** of a surveillance device includes use of the device:

- 23 (a) to listen to, record, observe or monitor the words, sounds or
24 signals communicated to or by a person, or the activities of a
25 person; or
26 (b) to track an object or person.

27 **8 Section 24**

28 Repeal the section, substitute:

1 **24 Exercise of authority under warrant etc.**

2 *Who may exercise authority under warrant etc.*

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

10 *Approval of persons authorised to exercise authority under*
11 *warrant etc.*

- 12 (2) The Director-General or a person appointed under subsection (3)
13 may, in writing, approve a person, or a class of persons, as people
14 authorised to exercise, on behalf of the Organisation, the authority
15 conferred by relevant warrants or relevant device recovery
16 provisions.
17 (3) The Director-General may, in writing, appoint a senior
18 position-holder, or a class of senior position-holders, for the
19 purposes of subsection (2).

20 *Definitions*

- 21 (4) In this section:

22 *relevant device recovery provision* means subsection 26B(5) or
23 (6), 27A(3A) or (3B) or 27F(5).

24 *relevant warrant* means a warrant issued under this Division or
25 under Division 3.

26 **9 Before section 25**

27 Insert:

28 **Subdivision B—Search warrants**

29 **10 After paragraph 25(4)(a)**

30 Insert:

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

3 **11 Paragraph 25(5)(a)**

4 After “adding,” insert “copying”.

5 **12 Subsection 25(6)**

6 Repeal the subsection, substitute:

7 *Certain acts not authorised*

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

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

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

18 **13 Subsection 25(7) (heading)**

19 Repeal the heading, substitute:

20 *Warrant must provide for certain matters*

21 **14 Paragraph 25(7)(a)**

22 After “any force”, insert “against persons and things”.

23 **15 Before section 25A**

24 Insert:

25 **Subdivision C—Computer access warrants**

26 **16 Subsection 25A(2)**

27 Omit “particular”.

28 **17 At the end of subsection 25A(2)**

29 Add:

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

2 **18 Subsection 25A(3)**

3 Repeal the subsection, substitute:

- 4 (3) The target computer may be any one or more of the following:
- 5 (a) a particular computer;
 - 6 (b) a computer on particular premises;
 - 7 (c) a computer associated with, used by or likely to be used by, a
 - 8 person (whose identity may or may not be known).

9 *Authorisation in warrant*

10 (3A) The warrant must:

- 11 (a) be signed by the Minister; and
- 12 (b) authorise the Organisation to do specified things, subject to
- 13 any restrictions or conditions specified in the warrant, in
- 14 relation to the target computer; and
- 15 (c) if the target computer is or includes a particular computer—
- 16 specify the computer; and
- 17 (d) if the target computer is or includes a computer on particular
- 18 premises—specify the premises; and
- 19 (e) if the target computer is or includes a computer associated
- 20 with, used by or likely to be used by, a person—specify the
- 21 person (whether by name or otherwise).

22 **19 After paragraph 25A(4)(aa)**

23 Insert:

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

26 **20 Subparagraph 25A(4)(a)(i)**

27 Omit “a computer”, substitute “the target computer”.

28 **21 Paragraph 25A(4)(a)**

29 After “access to data”, insert “(the *relevant data*)”.

30 **22 Paragraph 25A(4)(a)**

31 After “adding,”, insert “copying,”.

1 **23 After paragraph 25A(4)(a)**

2 Insert:

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

10 **24 Subsection 25A(4) (note)**

11 Omit “the target computer etc.”, substitute “a computer etc.”.

12 **25 Subsection 25A(5)**

13 Repeal the subsection, substitute:

14 *Certain acts not authorised*

- 15 (5) Subsection (4) does not authorise the addition, deletion or
16 alteration of data, or the doing of any thing, that is likely to:
17 (a) materially interfere with, interrupt or obstruct a
18 communication in transit or the lawful use by other persons
19 of a computer unless the addition, deletion or alteration, or
20 the doing of the thing, is necessary to do one or more of the
21 things specified in the warrant; or
22 (b) cause any other material loss or damage to other persons
23 lawfully using a computer.

24 **26 Subsection 25A(5A) (heading)**

25 Repeal the heading, substitute:

26 *Warrant must provide for certain matters*

27 **27 Paragraph 25A(5A)(a)**

28 After “any force”, insert “against persons and things”.

29 **28 Paragraph 25A(5A)(b)**

30 Before “state whether”, insert “if the warrant authorises entering
31 premises—”.

1 **29 Sections 26 to 26C**

2 Repeal the sections, substitute:

3 **Subdivision D—Use of surveillance devices**

4 **26 Issue of surveillance device warrants**

5 *Issue of surveillance device warrant*

- 6 (1) If the Director-General requests the Minister to do so, and the
7 Minister is satisfied as mentioned in subsection (3), the Minister
8 may issue a warrant in accordance with this section.
- 9 (2) The warrant may be issued:
- 10 (a) in relation to one or more of the following:
- 11 (i) a particular person;
- 12 (ii) particular premises;
- 13 (iii) an object or class of object; and
- 14 (b) in respect of more than one kind of surveillance device; and
- 15 (c) in respect of more than one surveillance device of any
16 particular kind.

17 *Test for issue of warrant*

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

- 1 (ii) the use on behalf of the Organisation of a surveillance
2 device in or on those premises will, or is likely to, assist
3 the Organisation in carrying out its function of obtaining
4 intelligence relevant to security; and
5 (c) if the warrant is requested in relation to an object or class of
6 object:
7 (i) that object, or an object of that class, is used or worn, or
8 likely to be used or worn by a person engaged in or
9 reasonably suspected by the Director-General of being
10 engaged in, or of being likely to engage in, activities
11 prejudicial to security; and
12 (ii) the use by the Organisation of a surveillance device in
13 or on that object, or an object of that class, will, or is
14 likely to, assist the Organisation in carrying out its
15 function of obtaining intelligence relevant to security.

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

19 *Warrant may be subject to restrictions or conditions*

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

22 **26A Requirements for surveillance device warrants**

- 23 (1) A surveillance device warrant must:
24 (a) be signed by the Minister; and
25 (b) specify:
26 (i) the kind of surveillance device, or kinds of surveillance
27 devices, authorised to be used; and
28 (ii) the date the warrant is issued; and
29 (iii) if the warrant is issued in relation to a particular
30 person—the name of the person (if known) or the fact
31 that the person's identity is unknown; and
32 (iv) if the warrant is issued in relation to particular
33 premises—the premises; and
34 (v) if the warrant is issued in relation to an object or class of
35 object—the object or class of object; and

- 1 (c) authorise the use of any force against persons and things that
2 is necessary and reasonable to do the things authorised by the
3 warrant; and
4 (d) state whether entry is authorised to be made at any time of
5 the day or night or during stated hours of the day or night.
- 6 (2) If a surveillance device warrant is issued in relation to particular
7 premises that are vehicles, the warrant need only specify the class
8 of vehicle in relation to which the use of the surveillance device is
9 authorised.
- 10 (3) The surveillance device warrant must specify the period during
11 which it is to remain in force. The period must not be more than 6
12 months, although the Minister may revoke the warrant before the
13 period has expired.
- 14 (4) Subsection (3) does not prevent the issue of any further warrant.

15 **26B What a surveillance device warrant authorises**

16 *Authorisation in warrant—particular person*

- 17 (1) If a surveillance device warrant is issued in relation to a particular
18 person, the warrant authorises the following:
- 19 (a) the installation, use and maintenance of a surveillance device
20 of the kind specified in the warrant to:
- 21 (i) listen to, record, observe or monitor the words, sounds
22 or signals communicated to or by the person, or the
23 activities of the person; or
24 (ii) track the person;
- 25 (b) the installation, use and maintenance of a surveillance device
26 of the kind specified in the warrant:
- 27 (i) in or on premises where the person is reasonably
28 believed to be or likely to be; or
29 (ii) in or on any other premises specified in the warrant
30 from which the activities of that person, or the words,
31 sounds or signals communicated by or to that person,
32 can be listened to, recorded, observed or monitored;
- 33 (c) entering the premises referred to in paragraph (b) for any of
34 the purposes referred to in paragraph (a) or (b) or in
35 subsection (4) or (5);

- 1 (d) the installation, use and maintenance of a surveillance device
2 of the kind specified in the warrant in or on any object used
3 or worn, or likely to be used or worn, by the person;
4 (e) the entry into or onto, or the alteration of, the object referred
5 to in paragraph (d);
6 (f) entering any premises in which the object referred to in
7 paragraph (d) is or is likely to be found, for any of the
8 purposes referred to in that paragraph or in subsection (4) or
9 (5);
10 (g) entering any other premises, for the purposes of gaining entry
11 to or exiting premises referred in to paragraph (b) or (f);
12 (h) any other thing reasonably incidental to any of the above.

13 *Authorisation in warrant—particular premises*

- 14 (2) If a surveillance device warrant is issued in relation to particular
15 premises (the **subject premises**), the warrant authorises the
16 following:
17 (a) the installation, use and maintenance of a surveillance device
18 of the kind specified in the warrant:
19 (i) in or on the subject premises; or
20 (ii) in or on any other premises specified in the warrant
21 from which the activities of a person, or the words,
22 sounds or signals communicated by or to a person, can
23 be listened to, recorded, observed or monitored while
24 the person is in or on the subject premises;
25 (b) entering the subject premises, or any other premises specified
26 in the warrant, for any of the purposes referred to in
27 paragraph (a) or subsection (4) or (5);
28 (c) entering any other premises, for the purposes of gaining entry
29 to or exiting the subject premises or any other premises
30 specified in the warrant;
31 (d) any other thing reasonably incidental to any of the above.

32 *Authorisation in warrant—object or class of object*

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

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

13 *Authorisation in warrant—general*

- 14 (4) A surveillance device warrant also authorises the following:
15 (a) the installation, use and maintenance of enhancement
16 equipment in relation to the surveillance device;
17 (b) the temporary removal of an object from premises for the
18 installation or maintenance of the surveillance device or
19 enhancement equipment and the return of the object to the
20 premises;
21 (c) the replacement of an object with an equivalent object for the
22 purposes of the installation or maintenance of the
23 surveillance device or enhancement equipment;
24 (d) the breaking open of any thing for the installation or
25 maintenance of the surveillance device or enhancement
26 equipment;
27 (e) the connection of the surveillance device or enhancement
28 equipment to any source of electricity and the use of
29 electricity from that source to operate the device or
30 equipment;
31 (f) the connection of the surveillance device or enhancement
32 equipment to any object or system that may be used to
33 transmit information in any form and the use of that object or
34 system in connection with the operation of the device or
35 equipment;
36 (g) the doing of any thing reasonably necessary to conceal the
37 fact that any thing has been done under the warrant;
38 (h) any other thing reasonably incidental to any of the above.
-

Recovery of surveillance devices

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38

- (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

1 (b) the surveillance device is a tracking device;
2 the Organisation is also authorised to use the surveillance device or
3 any enhancement equipment in relation to the device solely for the
4 purposes of the location and recovery of the device or equipment.

5 **26C Use etc. of listening device without warrant**

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

- 7 (a) an ASIO employee acting in the course of the ASIO
8 employee's duties;
9 (b) an ASIO affiliate acting in accordance with the contract,
10 agreement or other arrangement under which the ASIO
11 affiliate is performing functions or services for the
12 Organisation;

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

- 17 (c) the first person is the communicator of the words, sounds or
18 signals; or
19 (d) the second person intends, or should reasonably expect, those
20 words, sounds or signals to be communicated to the first
21 person, or to a class or group of persons in which the first
22 person is included; or
23 (e) the first person does so with the implied or express consent of
24 a person who is permitted under paragraph (c) or (d) to listen
25 to or record the words, sounds or signals.

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

28 **26D Use etc. of optical surveillance device without warrant**

29 Either of the following:

- 30 (a) an ASIO employee acting in the course of the ASIO
31 employee's duties;
32 (b) an ASIO affiliate acting in accordance with the contract,
33 agreement or other arrangement under which the ASIO
34 affiliate is performing functions or services for the
35 Organisation;

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

- 4 (c) entering premises without permission from the owner or
5 occupier of the premises; or
6 (d) interference with any vehicle or thing without permission of
7 the person having lawful possession or control of the vehicle
8 or thing.

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

11 **26E Use etc. of tracking device without warrant**

12 (1) Either of the following:

- 13 (a) an ASIO employee acting in the course of the ASIO
14 employee's duties;
15 (b) an ASIO affiliate acting in accordance with the contract,
16 agreement or other arrangement under which the ASIO
17 affiliate is performing functions or services for the
18 Organisation;

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

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

24 (2) Either of the following:

- 25 (a) an ASIO employee acting in the course of the ASIO
26 employee's duties;
27 (b) an ASIO affiliate, acting in accordance with the contract,
28 agreement or other arrangement under which the ASIO
29 affiliate is performing functions or services for the
30 Organisation;

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

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

1 **26F Director-General may determine that certain provisions do not**
2 **apply to specified ASIO affiliates**

- 3 (1) The Director-General may, by signed writing, determine that
4 section 26C or 26D or subsection 26E(1) or (2) does not apply to:
5 (a) a specified ASIO affiliate; or
6 (b) a specified class of ASIO affiliates.
- 7 (2) A determination under subsection (1) has effect accordingly.
- 8 (3) A determination under subsection (1) is not a legislative
9 instrument.
- 10 (4) The Director-General may, by signed writing, delegate the
11 Director-General's power under this section to:
12 (a) a Deputy Director-General; or
13 (b) any other ASIO employee or ASIO affiliate who holds, or is
14 acting in, a position in the Organisation that is equivalent to
15 or higher than a position occupied by an SES employee with
16 a classification of SES Band 2.
- 17 (5) In exercising powers under a delegation, the delegate must comply
18 with any written direction given by the Director-General to the
19 delegate.

20 **30 Before section 27**

21 Insert:

22 **Subdivision E—Inspection of postal and other articles**

23 **31 Subsection 27(1)**

24 Omit “this section or section 27A”, substitute “this Division”.

25 **32 Before section 27A**

26 Insert:

27 **Subdivision F—Foreign intelligence**

28 **33 Paragraph 27A(1)(a)**

29 Omit “computer or a thing”, substitute “computer or an object”.

1 **34 Paragraph 27A(1)(a)**

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

3 **35 Subsection 27A(1)**

4 Omit “those things”, substitute “those objects”.

5 **36 Paragraph 27A(2)(a)**

6 After “any force”, insert “against persons and things”.

7 **37 Paragraph 27A(2)(b)**

8 Before “state whether”, insert “if the warrant authorises entering
9 premises—”.

10 **38 Paragraph 27A(3)(b)**

11 Omit “26(3) or (4), 26B(3), 26C(3)”, substitute “26B(1), (2), (3) or (4)”.

12 **39 Subsections 27A(3A) and (3B)**

13 Repeal the subsections, substitute:

- 14 (3A) If a surveillance device is installed or used in accordance with a
15 warrant under this section authorising the doing of acts referred to
16 in subsection 26B(1) (2), (3) or (4), the Organisation is authorised
17 to do any of the following:
- 18 (a) recover the surveillance device or any enhancement
19 equipment in relation to the device;
 - 20 (b) enter any premises where the surveillance device is
21 reasonably believed to be, for the purpose of recovering the
22 device or the equipment;
 - 23 (c) enter any other premises for the purposes of gaining entry to
24 or exiting the premises referred to in paragraph (b);
 - 25 (d) enter into or onto, or alter, an object for the purpose of
26 recovering the device or the equipment;
 - 27 (e) replace an object with an equivalent object for the purposes
28 of recovering the device or the equipment;
 - 29 (f) break open any thing for the purpose of recovering the device
30 or the equipment;
 - 31 (g) if the device or equipment is installed in or on an object—
32 temporarily remove the object from any place where it is

- 1 situated for the purpose of recovering the device or the
2 equipment and returning the object to that place;
- 3 (h) use a nominal amount of electricity from any source to power
4 the device or equipment;
- 5 (i) any thing reasonably necessary to conceal the fact that any
6 thing has been done under this subsection;
- 7 (j) use any force against persons and things that is necessary and
8 reasonable to do any of the above;
- 9 (k) any other thing reasonably incidental to any of the above;
- 10 at the following time:
- 11 (l) at any time while the warrant is in force or within 28 days
12 after it ceases to be in force;
- 13 (m) if the surveillance device is not recovered at a time
14 mentioned in paragraph (l)—at the earliest time, after the 28
15 days mentioned in that paragraph, at which it is reasonably
16 practicable to do the things concerned.
- 17 (3B) If, for the purposes of subsection (3A):
- 18 (a) the surveillance device is not recovered while the warrant is
19 in force; and
- 20 (b) the surveillance device is a tracking device;
- 21 the Organisation is also authorised to use the surveillance device or
22 any enhancement equipment in relation to the device solely for the
23 purposes of the location and recovery of the device or equipment.

24 **40 Subsection 27A(5)**

25 Repeal the subsection.

26 **41 After section 27B**

27 Insert:

28 **Subdivision G—Identified person warrants**

29 **27C Issue of identified person warrants**

30 *Issue of warrant*

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

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

3 *Test for issue of warrant*

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

12 *Requirements for warrant*

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

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

32 *Duration of warrant*

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

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

3 *Issue of further warrants not prevented*

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

5 *Warrant may be subject to restrictions or conditions*

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

8 **27D Authority under identified person warrant—search of premises**
9 **and persons**

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

13 *Things that may be authorised under warrant*

14 (2) Subject to subsection (3), the Minister or the Director-General
15 may, on request, authorise the Organisation to do one or more of
16 the following things under the identified person warrant in relation
17 to one or more specified premises (the *subject premises*):

18 (a) enter the subject premises;

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

21 (c) search the subject premises for the purpose of finding records
22 or other things relevant to the prejudicial activities of the
23 identified person;

24 (d) open any safe, box, drawer, parcel, envelope or other
25 container in or on the premises in which there is reasonable
26 cause to believe that records or other things relevant to the
27 prejudicial activities of the identified person may be found;

28 (e) conduct an ordinary search or a frisk search of the identified
29 person or any other person if:

30 (i) the person is at or near the subject premises when the
31 authority given by this subsection is exercised; and

32 (ii) there is reasonable cause to believe that the person has,
33 on his or her person, records or other things that are

- 1 relevant to the prejudicial activities of the identified
2 person;
- 3 (f) inspect or otherwise examine any records or other things so
4 found, and make copies or transcripts of any such record or
5 other thing that appears to be relevant to the collection of
6 intelligence by the Organisation in accordance with this Act;
- 7 (g) remove and retain any record or other thing so found, for the
8 purposes of:
- 9 (i) inspecting or examining it; and
10 (ii) making copies or transcripts of it;
- 11 (h) if there is reasonable cause to believe that data relevant to the
12 prejudicial activities of the identified person may be
13 accessible by using a computer or other electronic equipment,
14 or a data storage device, brought to or found on the subject
15 premises—use the computer, equipment or device for the
16 purpose of obtaining access to any such data and, if necessary
17 to achieve that purpose, add, copy, delete or alter other data
18 in the computer, equipment or device;
- 19 (i) if paragraph (h) applies—use the computer, equipment or
20 device to do any of the following:
- 21 (i) inspect and examine any data to which access has been
22 obtained;
- 23 (ii) convert any data to which access has been obtained, that
24 appears to be relevant to the collection of intelligence by
25 the Organisation in accordance with this Act, into
26 documentary form and removing any such document;
- 27 (iii) copy any data to which access has been obtained, that
28 appears to be relevant to the collection of intelligence by
29 the Organisation in accordance with this Act, to any
30 data storage device and remove the device;
- 31 (j) any thing reasonably necessary to conceal the fact that any
32 thing has been done under the warrant;
- 33 (k) any other thing reasonably incidental to any of the above.

34 *Test for authorisation*

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

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

4 *Additional rules applying to authorisations*

- 5 (4) An ordinary search or frisk search of a person that is authorised
6 under paragraph (2)(e) must, if practicable, be conducted by a
7 person of the same sex as the person being searched.
- 8 (5) A record or other thing retained as mentioned in paragraph (2)(g)
9 may be retained:
- 10 (a) if returning the record or thing would be prejudicial to
11 security—only until returning the record or thing would no
12 longer be prejudicial to security; and
13 (b) otherwise—for only such time as is reasonable.

14 *Certain acts not authorised*

- 15 (6) Paragraph (2)(e) does not authorise a strip search or a search of a
16 person's body cavities.
- 17 (7) Paragraphs (2)(h) to (k) do not authorise the addition, deletion or
18 alteration of data, or the doing of any thing, that is likely to:
- 19 (a) materially interfere with, interrupt or obstruct the lawful use
20 by other persons of a computer or other electronic equipment,
21 or a data storage device, found on the subject premises unless
22 the addition, deletion or alteration, or the doing of the thing,
23 is necessary to do the things authorised under one or more of
24 those paragraphs; or
25 (b) cause any other material loss or damage to other persons
26 lawfully using the computer, equipment or device.

27 **27E Authority under identified person warrant—computer access**

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

31 *Things that may be authorised under warrant*

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

- 1 the following things under the identified person warrant in relation
2 to a computer (the *target computer*):
- 3 (a) enter specified premises for the purposes of doing the things
4 authorised under this subsection;
 - 5 (b) enter any premises for the purposes of gaining entry to or
6 exiting the specified premises;
 - 7 (c) use:
 - 8 (i) the target computer; or
 - 9 (ii) a telecommunications facility operated or provided by
10 the Commonwealth or a carrier; or
 - 11 (iii) any other electronic equipment; or
 - 12 (iv) a data storage device;
 - 13 for the purpose of obtaining access to data (the *relevant data*)
14 that is relevant to the prejudicial activities of the identified
15 person and is held in the target computer at any time while
16 the authorisation is in force and, if necessary to achieve that
17 purpose, add, copy, delete or alter other data in the target
18 computer;
 - 19 (d) if, having regard to other methods (if any) of obtaining access
20 to the relevant data which are likely to be as effective, it is
21 reasonable in all the circumstances to do so—use any other
22 computer or a communication in transit for the purpose
23 referred to in paragraph (c) and, if necessary to achieve that
24 purpose, add, copy, delete or alter other data in the computer
25 or the communication in transit;
 - 26 (e) copy any data to which access has been obtained, that
27 appears to be relevant to the collection of intelligence by the
28 Organisation in accordance with this Act;
 - 29 (f) any thing reasonably necessary to conceal the fact that any
30 thing has been done under the warrant;
 - 31 (g) any other thing reasonably incidental to any of the above.

32 *Target computer*

- 33 (3) For the purposes of subsection (2), the target computer may be any
34 one or more of the following:
- 35 (a) a particular computer;
 - 36 (b) a computer on particular premises;

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

3 *Test for authorisation*

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

10 *Certain acts not authorised*

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

20 **27F Authority under identified person warrant—surveillance**
21 **devices**

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

25 *Things that may be authorised under warrant*

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

- 1 (b) install, use and maintain surveillance devices of the kind
2 specified in the conditional approval:
3 (i) in or on premises where the identified person is
4 reasonably believed to be or likely to be; or
5 (ii) in or on any other specified premises from which the
6 activities of the identified person, or the words, sounds
7 or signals communicated by or to the identified person,
8 can be listened to, recorded, observed or monitored;
9 (c) enter the premises referred to in paragraph (b) for any of the
10 purposes referred to in paragraph (a) or (b) or in
11 subsection 26B(4), (5) or (6) (as those subsections apply
12 because of this section);
13 (d) install, use and maintain surveillance devices of the kind
14 specified in the conditional approval in or on any object used
15 or worn, or likely to be used or worn, by the identified
16 person;
17 (e) enter into or onto, or alter, an object referred to in
18 paragraph (d);
19 (f) enter any premises in which an object referred to in
20 paragraph (d) is or is likely to be found, for any of the
21 purposes referred to in that paragraph or in
22 subsection 26B(4), (5) or (6) (as those subsections apply
23 because of this section);
24 (g) enter any other premises, for the purposes of gaining entry to
25 or exiting premises referred to in paragraph (b) or (f);
26 (h) any other thing reasonably incidental to any of the above.

27 *Test for authorisation*

- 28 (3) The Minister or the Director-General is only to give an
29 authorisation under subsection (2) if the Minister or the
30 Director-General is satisfied, on reasonable grounds, that doing
31 that thing or those things under the warrant will substantially assist
32 the collection of intelligence relevant to the prejudicial activities of
33 the identified person.
34 (4) If an authorisation is given under subsection (2) in relation to a
35 surveillance device, the identified person warrant under which the
36 authorisation is given also authorises the Organisation to do the
37 things mentioned in subsection 26B(4) in relation to the device.

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

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

8 **27G Authority under identified person warrant—inspection of**
9 **postal articles**

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

14 *Things that may be authorised under warrant*

15 (2) Subject to subsection (4), the Minister or the Director-General
16 may, on request, authorise the Organisation to do one or more of
17 the things mentioned in subsection (3) under the identified person
18 warrant in relation to any of the following:

- 19 (a) articles posted by or on behalf of the identified person;
20 (b) articles addressed to the identified person;
21 (c) articles reasonably suspected by a person authorised to
22 exercise the authority of the Organisation under the warrant
23 to be intended to be received by the identified person.

24 (3) The things are as follows:

- 25 (a) inspect and make copies of the articles, or the covers of the
26 articles;
27 (b) open the articles;
28 (c) inspect and make copies of the contents of the articles;
29 (d) any other thing reasonably incidental to any of the above.

30 *Test for authorisation*

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

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

3 *Rules relating to the Australian Postal Corporation*

4 (5) If an authorisation is given under this section, the Director-General
5 must, as soon as practicable:

6 (a) inform the Australian Postal Corporation of that fact; and

7 (b) give a certified copy of the authorisation to the Australian
8 Postal Corporation.

9 (6) If either of the following is revoked:

10 (a) an authorisation under this section;

11 (b) the identified person warrant under which the authorisation is
12 given;

13 the Director-General must:

14 (c) inform the Australian Postal Corporation of that fact; and

15 (d) give a certified copy of the instrument of revocation to the
16 Australian Postal Corporation.

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

20 *Relationship with other laws*

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

24 **27H Authority under identified person warrant—inspection of**
25 **delivery articles**

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

30 *Things that may be authorised under warrant*

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

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

- 3 (a) articles posted by or on behalf of the identified person;
- 4 (b) articles addressed to the identified person;
- 5 (c) articles reasonably suspected by a person authorised to
6 exercise the authority of the Organisation under the warrant
7 to be intended to be received by the identified person.

8 (3) The things are as follows:

- 9 (a) inspect and make copies of the articles, or the covers of the
10 articles;
- 11 (b) open the articles;
- 12 (c) inspect and make copies of the contents of the articles;
- 13 (d) any other thing reasonably incidental to any of the above.

14 *Test for authorisation*

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

21 *Definitions*

22 (5) In this section:

23 *article* has the same meaning as in section 27AA.

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

26 **27J Authority under identified person warrants—general rules**

27 *Requests for authorisations*

28 (1) A request for an authorisation under this Subdivision may be made:
29 (a) if the request is to the Minister—by the Director-General; or
30 (b) if the request is to the Director-General—by an ASIO
31 employee or an ASIO affiliate.

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

4 *Requirements for authorisations*

- 5 (3) An authorisation under this Subdivision:
6 (a) must be in writing; and
7 (b) must identify the identified person warrant under which the
8 authorisation is given; and
9 (c) must specify:
10 (i) for an authorisation under section 27D (search of
11 premises or persons)—the subject premises; and
12 (ii) for an authorisation under section 27E (computer
13 access)—the target computer; and
14 (iii) the thing or things that are authorised to be done; and
15 (iv) the restrictions or conditions (if any) to which the
16 authorisation is subject; and
17 (v) the period during which the authorisation is in force;
18 and
19 (d) must authorise the use of any force against persons and
20 things that is necessary and reasonable to do the things
21 covered by the authorisation; and
22 (e) if the authorisation authorises entering premises—must state
23 whether entry is authorised to be made at any time of the day
24 or night or during stated hours of the day or night.
- 25 (4) A restriction or condition specified in an authorisation must not be
26 inconsistent with any restrictions or conditions specified in the
27 identified person warrant under which the authorisation is given.
- 28 (5) For the purposes of subparagraph (3)(c)(v), the period:
29 (a) in the case of an authorisation under section 27D (search of
30 premises and persons)—must not be more than 90 days; and
31 (b) in any case—must not end after the end of the period for
32 which the identified person warrant under which the
33 authorisation is given is in force.

1 *When authorisations cease to be in force*

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

8 *Other matters*

- 9 (7) To avoid doubt, for the purposes of this Act, the authority
10 conferred by an identified person warrant includes the authority
11 conferred by an authorisation under this Subdivision under the
12 warrant.
13 (8) To avoid doubt, nothing in this Subdivision prevents 2 or more
14 authorisations under this Subdivision from being given under the
15 same identified persons warrant at any time while the warrant is in
16 force.
17 (9) An authorisation under this Subdivision is not a legislative
18 instrument.

19 **42 Before section 28**

20 Insert:

21 **Subdivision H—General provisions relating to warrants**

22 **43 Paragraph 29(1)(a)**

23 Omit “26B, 26C.”.

24 **44 After section 29**

25 Insert:

26 **29A Variation of warrants issued under this Division**

- 27 (1) The Minister may, on request by the Director-General, vary a
28 warrant issued under this Division (other than under section 29).
29 (2) The variation must be in writing.

- 1 (3) If the variation extends, or further extends, the period during which
2 the warrant is in force, the total period during which the warrant is
3 in force must not exceed:
4 (a) for a warrant issued under section 25—90 days; or
5 (b) for a warrant issued under section 25A, 26, 27, 27AA or
6 27C—6 months.
- 7 (4) The request by the Director-General must specify:
8 (a) the facts and other grounds on which the Director-General
9 considers it necessary that the warrant should be varied; and
10 (b) where appropriate—the grounds on which the
11 Director-General suspects a person of being engaged in or
12 reasonably suspected by the Director-General of being
13 engaged in, or of being likely to engage in, activities
14 prejudicial to security.
- 15 (5) A warrant may be varied more than once under this section.

16 **45 Section 30**

17 Repeal the section, substitute:

18 **30 Discontinuance of action before expiration of warrant**

- 19 (1) Subject to subsection (3), if the Director-General is satisfied that
20 the grounds on which a warrant under this Division was issued
21 have ceased to exist, the Director-General must, as soon as
22 practicable:
23 (a) inform the Minister of that fact; and
24 (b) take such steps as are necessary to ensure that action under
25 the warrant is discontinued.
- 26 (2) For the purposes of paragraph (1)(b), *action under a warrant*:
27 (a) includes action under an authorisation given under an
28 identified person warrant; but
29 (b) does not include the recovery of a surveillance device or any
30 enhancement equipment in relation to the device.
- 31 (3) If:
32 (a) a surveillance device warrant was issued in relation to more
33 than one of the matters mentioned in paragraph 26(2)(a); and

- 1 (b) the grounds on which the warrant was issued continue to
2 exist for at least one of those matters;
3 subsection (1) applies only in relation to the matters for which the
4 grounds have ceased to exist.

5 **46 After section 32**

6 Insert:

7 **33 Relationship with other laws**

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

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

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

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

25 *Surveillance devices—interaction with other laws*

- 26 (3) Despite any other law of the Commonwealth, a State or a Territory
27 (including the common law), a person acting on behalf of the
28 Organisation does not act unlawfully by installing, using or
29 maintaining a surveillance device if the person does so:
30 (a) in accordance with a warrant issued under section 26, 27A or
31 27C; or
32 (b) in accordance with subsection 26B(5) or (6), section 26C,
33 26D, or 26E, or subsection 27A(3A) or (3B) or 27F(5).

1 **47 At the end of Division 2 of Part III**

2 Add:

3 **34AA Evidentiary certificates**

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

- 10 (2) A certificate may be issued with respect to acts or things done in
11 connection with:
12 (a) a warrant issued under section 27A or 29, but only if the
13 warrant authorises the doing of acts or things referred to in
14 section 25A or 26B, and only with respect to those acts or
15 things; or
16 (b) a warrant issued under section 27C, but only if acts or things
17 are authorised under section 27E or 27F under the warrant,
18 and only with respect to those acts or things.

- 19 (3) Without limiting subsection (1), the certificate may set out one or
20 more of the following:
21 (a) if premises were entered under the relevant warrant or
22 relevant authorising provision:
23 (i) details of the premises; or
24 (ii) the time of day or night the premises were entered;
25 (b) if data was accessed under the relevant warrant or relevant
26 authorising provision—details of the computer,
27 telecommunications facility, electronic equipment, data
28 storage device or communication in transit used for the
29 purpose of obtaining such access;
30 (c) if the warrant is a surveillance device warrant—the matters
31 required to be specified under section 26A for the warrant;
32 (d) if one or more surveillance devices were installed, used or
33 maintained under the relevant warrant or relevant authorising
34 provision:
35 (i) details of the installation, use or maintenance of the
36 surveillance device or devices; or

- 1 (ii) details of the installation, use or maintenance of any
2 enhancement equipment in relation to the surveillance
3 device; or
4 (iii) details of the processes and procedures employed to use
5 the surveillance device or devices, or any enhancement
6 equipment; or
7 (iv) details of acts or things done for the purposes of
8 recovering the surveillance device or devices, or any
9 enhancement equipment;
10 (e) details of things done under the relevant warrant or relevant
11 authorising provision that were reasonably necessary to
12 conceal the fact that things were done under the relevant
13 warrant or relevant authorising provision;
14 (f) details of persons who exercised the authority given by the
15 relevant warrant or relevant authorising provision;
16 (g) details of things done under the relevant warrant or relevant
17 authorising provision that were reasonably incidental to any
18 of the acts or things done by, on behalf of, or in relation to,
19 the Organisation in connection with the relevant warrant or
20 relevant authorising provision.

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

23 (5) In this section:

24 ***proceeding*** means:

- 25 (a) a proceeding or proposed proceeding in a federal court, or in
26 a court of a State or Territory; or
27 (b) a proceeding or proposed proceeding (including a hearing or
28 examination, or proposed hearing or examination) by or
29 before:
30 (i) a tribunal in Australia; or
31 (ii) any other body, authority or person in Australia having
32 power to hear or examine evidence.

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

35 ***relevant warrant*** means a warrant issued under section 25A, 26,
36 27A, 27C or 29.

1 **Part 2—Consequential amendments**

2 ***Telecommunications (Interception and Access) Act 1979***

3 **48 After paragraph 108(2)(c)**

4 Insert:

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

8 **49 At the end of paragraph 108(2)(f)**

9 Add:

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

1 **Part 3—Application, transitional and savings**
2 **provisions**

3 **50 Application, transitional and savings provisions**

- 4 (1) Subject to this item, the amendments made by this Schedule do not
5 apply in relation to:
- 6 (a) warrants requested before the commencement of this
7 Schedule; or
8 (b) warrants issued before the commencement of this Schedule.
- 9 (2) If, immediately before the commencement of this Schedule, a person
10 was approved under subsection 24(1) of the *Australian Security*
11 *Intelligence Organisation Act 1979*, the person is taken, after that
12 commencement, to be a person approved under subsection 24(2) of that
13 Act as amended by this Schedule.
- 14 (3) If, immediately before the commencement of this Schedule, a person
15 was an authorising officer for the purposes of subsection 24(1) of the
16 *Australian Security Intelligence Organisation Act 1979*, the person is
17 taken, after that commencement, to be a person appointed under
18 subsection 24(3) of that Act as amended by this Schedule.
- 19 (4) Section 34AA of the *Australian Security Intelligence Organisation Act*
20 *1979*, as inserted by this Schedule, applies in relation to:
- 21 (a) warrants issued, and authorisations given, after the
22 commencement of this Schedule; and
23 (b) proceedings commenced after that commencement.

1 **Schedule 3—Protection for special**
2 **intelligence operations**
3

4 *Australian Security Intelligence Organisation Act 1979*

5 **1 Section 4**

6 Insert:

7 *authorising officer* means:

- 8 (a) the Director-General; or
9 (b) a Deputy Director-General.

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

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

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

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

21 *special intelligence operation* is an operation:

- 22 (a) in relation to which a special intelligence operation authority
23 has been granted; and
24 (b) that is carried out for a purpose relevant to the performance
25 of one or more special intelligence functions; and
26 (c) that may involve an ASIO employee or an ASIO affiliate in
27 special intelligence conduct.

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

30 **2 Subsection 34ZF(8)**

31 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) An ASIO employee may apply to an authorising officer 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.

- 1 (4) As soon as practicable after making an application in accordance
2 with paragraph (2)(b), the applicant must:
3 (a) make a written record of the application; and
4 (b) give a copy of it to the authorising officer to whom the
5 application was made.

6 **35C Granting of special intelligence operation authorities**

- 7 (1) If:
8 (a) an application for an authority to conduct a special
9 intelligence operation is made under section 35B; and
10 (b) the authorising officer to whom the application was made is
11 satisfied on reasonable grounds of the matters in
12 subsection (2);
13 the authorising officer may authorise the special intelligence
14 operation by granting the authority.
- 15 (2) The matters are as follows:
16 (a) the special intelligence operation will assist the Organisation
17 in the performance of one or more special intelligence
18 functions;
19 (b) the circumstances are such as to justify the conduct of a
20 special intelligence operation;
21 (c) any unlawful conduct involved in conducting the special
22 intelligence operation will be limited to the maximum extent
23 consistent with conducting an effective special intelligence
24 operation;
25 (d) the special intelligence operation will not be conducted in
26 such a way that a person is likely to be induced to commit an
27 offence against a law of the Commonwealth, a State or a
28 Territory that the person would not otherwise have intended
29 to commit;
30 (e) any conduct involved in the special intelligence operation
31 will not:
32 (i) cause the death of, or serious injury to, any person; or
33 (ii) involve the commission of a sexual offence against any
34 person; or
35 (iii) result in significant loss of, or serious damage to,
36 property.

-
- 1 (3) A special intelligence operation authority may be granted
2 unconditionally or subject to conditions.
- 3 (4) A special intelligence operation authority may be granted:
4 (a) by means of a written document signed by the authorising
5 officer; or
6 (b) if the authorising officer reasonably believes that the delay
7 caused by giving a written authority may be prejudicial to
8 security—orally in person, or by telephone or other means of
9 communication.
- 10 (5) If a special intelligence operation authority is granted in
11 accordance with paragraph (4)(b), the authorising officer must,
12 within 7 days, issue a written record of the special intelligence
13 operation authority that complies with section 35D.
- 14 (6) To avoid doubt, nothing in this Division prevents a special
15 intelligence operation authority being granted in respect of a
16 special intelligence operation that has been the subject of a
17 previous special intelligence operation authority.
- 18 Note: A special intelligence operation authority can be varied, but not so as
19 to extend beyond 12 months—see section 35F.
- 20 (7) The following are not legislative instruments:
21 (a) a document referred to in paragraph (4)(a);
22 (b) a written record referred to in subsection (5).

23 **35D Contents of special intelligence operation authorities**

- 24 (1) A special intelligence operation authority must:
25 (a) state how the special intelligence operation will assist the
26 Organisation in the performance of one or more special
27 intelligence functions; and
28 (b) identify the persons authorised to engage in special
29 intelligence conduct for the purposes of the special
30 intelligence operation; and
31 (c) state a general description of the nature of the special
32 intelligence conduct that the persons referred to in
33 paragraph (b) may engage in; and

- 1 (d) specify the period of effect of the special intelligence
2 operation authority, being a period not exceeding 12 months;
3 and
4 (e) specify any conditions to which the conduct of the special
5 intelligence operation is subject; and
6 (f) state the date and time when the special intelligence
7 operation authority is granted.

- 8 (2) A person is sufficiently identified for the purposes of
9 paragraph (1)(b) if the person is identified:
10 (a) by an assumed name under which the person is operating; or
11 (b) by a code name or code number;
12 as long as the authorising officer can match the assumed name,
13 code name or code number to the person's identity.

14 **35E Commencement and duration of special intelligence operation**
15 **authorities**

- 16 (1) A special intelligence operation authority comes into force at the
17 time the special intelligence operation authority is granted under
18 section 35C.
19 (2) A special intelligence operation authority has effect for the period
20 specified in accordance with paragraph 35D(1)(d) unless:
21 (a) it is cancelled before the end of the period of effect; or
22 (b) the period of effect is extended under section 35F.

23 **35F Variation of special intelligence operation authorities**

- 24 (1) An authorising officer may vary a special intelligence operation
25 authority:
26 (a) at any time on the authorising officer's own initiative; or
27 (b) on application by an ASIO employee.

28 *Application for variation*

- 29 (2) An application under paragraph (1)(b) may be made:
30 (a) in writing signed by the applicant; or
31 (b) if the applicant reasonably believes that the delay caused by
32 making a written application may be prejudicial to security—

1 orally in person, or by telephone or other means of
2 communication.

- 3 (3) As soon as practicable after making an application in accordance
4 with paragraph (1)(b), the applicant must:
5 (a) make a written record of the application; and
6 (b) give a copy of it to the authorising officer to whom the
7 application was made.

8 *Limits on variation*

- 9 (4) The authorising officer must not vary the special intelligence
10 operation authority unless the authorising officer:
11 (a) is satisfied on reasonable grounds that the special intelligence
12 operation, conducted in accordance with the special
13 intelligence operation authority as varied, will assist the
14 Organisation in the performance of one or more special
15 intelligence functions; and
16 (b) considers it appropriate to do so.
- 17 (5) If a variation extends, or further extends, the period of effect of a
18 special intelligence operation authority, the total period of effect
19 must not be longer than 12 months.

20 *Manner of variation*

- 21 (6) The variation may be made:
22 (a) by means of a written document signed by the authorising
23 officer; or
24 (b) if the authorising officer reasonably believes that the delay
25 caused by giving a written variation may be prejudicial to
26 security—orally in person, or by telephone or other means of
27 communication.
- 28 (7) If a special intelligence operation authority is varied in accordance
29 with paragraph (6)(b), the authorising officer must, within 7 days,
30 issue a written record of the variation, signed by the authorising
31 officer.

1 *Authority may be varied more than once*

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

4 **35G Cancellation of special intelligence operation authorities**

5 (1) An authorising officer may cancel a special intelligence operation
6 authority at any time and for any reason.

7 (2) A cancellation of a special intelligence operation authority must:

8 (a) be in writing; and

9 (b) specify when the cancellation takes effect.

10 **35H Effect of special intelligence operation authorities**

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

15 (2) The authorisation, in relation to a person identified in the special
16 intelligence operation authority, is for the period of effect of the
17 special intelligence operation authority, unless:

18 (a) the special intelligence operation authority specifies a shorter
19 period during which the person is so authorised; or

20 (b) the special intelligence operation authority is varied under
21 section 35F to provide that the person is no longer so
22 authorised; or

23 (c) the special intelligence operation authority is cancelled
24 before the end of that period.

25 **35J Defect in a special intelligence operation authority**

26 An application for a special intelligence operation authority or
27 variation of such an authority, and any special intelligence
28 operation authority or variation of such an authority granted on the
29 basis of such an application, is not invalidated by any defect, other
30 than a defect that affects the application, special intelligence
31 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
 - (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

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

5 (3) This section is enacted to avoid doubt.

6 **35M Effect of being unaware of variation or cancellation of special**
7 **intelligence operation authority**

- 8 (1) If an authority to conduct a special intelligence operation is varied
9 in a way that limits its scope, this Division continues to apply to a
10 participant in the special intelligence operation as if the authority
11 had not been varied in that way, for so long as the participant:
12 (a) is unaware of the variation; and
13 (b) is not reckless about the existence of the variation.
- 14 (2) If an authority to conduct a special intelligence operation is
15 cancelled, this Division continues to apply to a person who was a
16 participant in the special intelligence operation immediately before
17 the cancellation as if the authority had not been cancelled in that
18 way, for so long as the person:
19 (a) is unaware of the cancellation; and
20 (b) is not reckless about the existence of the cancellation.
- 21 (3) For the purposes of this section, a person is reckless about the
22 existence of the variation or cancellation of a special intelligence
23 operation authority if:
24 (a) the person is aware of a substantial risk that the variation or
25 cancellation has happened; and
26 (b) having regard to the circumstances known to the person, it is
27 unjustifiable to take the risk that the special intelligence
28 operation authority has not been varied or cancelled.

29 **35N Protection from criminal responsibility for certain ancillary**
30 **conduct**

- 31 (1) This section applies if:
32 (a) a person engages in conduct (the *ancillary conduct*) that
33 relates to special intelligence conduct (the *related conduct*)
34 engaged in by another person; and
-

- 1 (b) engaging in the ancillary conduct is an ancillary offence in
 2 relation to the offence constituted by the related conduct.
- 3 (2) Despite any other law of the Commonwealth, a State or a Territory,
 4 the person who engaged in the ancillary conduct is not criminally
 5 responsible for the ancillary offence, if, at the time the person
 6 engaged in the ancillary conduct, he or she believed the related
 7 conduct was being engaged in, or would be engaged in, by a
 8 participant in a special intelligence operation authorised under this
 9 Division.
- 10 (3) For the purposes of this section, *ancillary offence*, in relation to an
 11 offence constituted by related conduct, means an offence against a
 12 law of the Commonwealth, a State or a Territory:
- 13 (a) of conspiring to commit the offence constituted by the related
 14 conduct; or
- 15 (b) of aiding, abetting, counselling or procuring, inciting or being
 16 in any way knowingly concerned in, the commission of the
 17 offence constituted by the related conduct.

18 **35P Unauthorised disclosure of information**

19 *Unauthorised disclosure of information*

- 20 (1) A person commits an offence if:
 21 (a) the person discloses information; and
 22 (b) the information relates to a special intelligence operation.

23 Penalty: Imprisonment for 5 years.

24 *Unauthorised disclosure of information—endangering safety, etc.*

- 25 (2) A person commits an offence if:
 26 (a) the person discloses information; and
 27 (b) the information relates to a special intelligence operation; and
 28 (c) either:
 29 (i) the person intends to endanger the health or safety of
 30 any person or prejudice the effective conduct of a
 31 special intelligence operation; or

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

4 Penalty: Imprisonment for 10 years.

5 *Exceptions*

- 6 (3) Subsections (1) and (2) do not apply if the disclosure was:
7 (a) in connection with the administration or execution of this
8 Division; or
9 (b) for the purposes of any legal proceedings arising out of or
10 otherwise related to this Division or of any report of any such
11 proceedings; or
12 (c) in accordance with any requirement imposed by law; or
13 (d) in connection with the performance of functions or duties, or
14 the exercise of powers, of the Organisation.

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

17 *Extended geographical jurisdiction*

- 18 (4) Section 15.4 of the *Criminal Code* (extended geographical
19 jurisdiction—category D) applies to an offence against
20 subsection (1) or (2).
21 (5) Subsection (4) does not, by implication, affect the interpretation of
22 any other provision of this Act.

23 **35Q Reports by the Director-General**

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

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

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

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

10 **35R Evidence relating to granting of special intelligence operation**
11 **authority**

12 (1) An authorising officer may issue a written certificate signed by the
13 authorising officer setting out such facts as the authorising officer
14 considers relevant with respect to the granting of a special
15 intelligence operation authority.

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

18 **4 After subsection 94(2)**

19 Insert:

20 (2A) A report under subsection (1) must also include a statement of:

- 21 (a) the total number of applications made under section 35B
22 during the year for the granting of special intelligence
23 operation authorities; and
24 (b) the total number of special intelligence operation authorities
25 granted during the year.

1 **Schedule 4—ASIO co-operation and**
2 **information sharing**
3

4 *Australian Security Intelligence Organisation Act 1979*

5 **1 Paragraph 18(3)(b)**

6 Omit “either”, substitute “any of the following subparagraphs apply”.

7 **2 Subparagraph 18(3)(b)(i)**

8 Omit “crime; or”, substitute “crime;”.

9 **3 After subparagraph 18(3)(b)(i)**

10 Insert:

- 11 (ia) the information relates, or appears to relate, to the
12 commission, or intended commission, of an offence
13 against section 92 (publication of identity of ASIO
14 employee or ASIO affiliate);

15 **4 At the end of paragraph 19(1)(a)**

16 Add “and”.

17 **5 At the end of subsection 19(1)**

18 Add:

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

20 **6 At the end of section 92**

21 Add:

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

24 **7 Application—communication of intelligence etc.**

25 The amendments of section 18 of the *Australian Security Intelligence*
26 *Organisation Act 1979* made by this Schedule apply in relation to
27 communications of information made on or after the commencement of
28 this Schedule, whether the information has come into the possession of
29 the Organisation before or after that commencement.

1 **Schedule 5—Activities and functions of**
2 **Intelligence Services Act 2001**
3 **agencies**
4

5 **1 Section 3**

6 Insert:

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

- 9 (a) interference by a foreign person or entity; or
10 (b) reliance on inaccurate or false information.

11 **2 Before section 6**

12 Insert:

13 **Division 1—Functions of the agencies**

14 **3 After paragraph 6(1)(da)**

15 Insert:

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

17 **4 Subparagraph 6B(e)(ii)**

18 Omit “such imagery or products”, substitute “imagery and other
19 geospatial products”.

20 **5 After subparagraph 6B(e)(ii)**

21 Insert:

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

24 **6 After subparagraph 9(1A)(a)(iii)**

25 Insert:

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

28 **7 Subsection 9(1B) (note)**

29 After “*crime*”, insert “and *operational security of ASIS*”.

1 **8 Before section 13**

2 Insert:

3 **Division 2—Co-operation**

4 **9 Subsection 13(1A)**

5 Omit all the words after “planning or”, substitute:

6 undertaking:

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

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

9 unless, before giving the approval, the Minister consults with the

10 Prime Minister and the Attorney-General.

11 **10 Application—subsection 13(1A)**

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

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

20 **11 After section 13A**

21 Insert:

22 **Division 3—Activities undertaken in relation to ASIO**

23 **13B Activities undertaken in relation to ASIO**

24 *When an activity may be undertaken in relation to ASIO*

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

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

-
- 1 (b) the activity or series of activities will be undertaken outside
 2 Australia; and
 3 (c) the activity or series of activities will be undertaken to
 4 support ASIO in the performance of its functions; and
 5 (d) either:
 6 (i) the Director-General of Security; or
 7 (ii) a person who is authorised under section 13C for the
 8 purposes of this subparagraph;
 9 has, in writing, notified ASIS that ASIO requires the
 10 production of intelligence on the Australian person or class of
 11 Australian persons.

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

15 *When notice from ASIO not required—particular activity*

- 16 (3) Paragraph (1)(d) does not apply in relation to the undertaking of a
 17 particular activity in relation to a particular Australian person if a
 18 staff member of ASIS who:
 19 (a) is authorised under subsection (7); and
 20 (b) will be undertaking the activity;
 21 reasonably believes that it is not practicable in the circumstances
 22 for ASIO to notify ASIS in accordance with that paragraph before
 23 undertaking the activity.

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

28 *Effect of this section*

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

32 *Incidental production of intelligence*

- 33 (6) An activity, or a series of activities, does not cease to be
 34 undertaken:

- 1 (a) in accordance with this section; or
2 (b) for the specific purpose of supporting ASIO in the
3 performance of its functions;
4 only because, in undertaking the activity or series of activities,
5 ASIS also incidentally produces intelligence that relates to the
6 involvement, or likely involvement, of an Australian person in one
7 or more of the activities set out in paragraph 9(1A)(a).

8 *Authorised staff members*

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

12 *Instruments not legislative instruments*

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

17 **13C Authorised persons for activities undertaken in relation to**
18 **ASIO**

19 *Authorised persons*

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

23 *Authorisation is not a legislative instrument*

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

26 *Definitions*

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

1 **13D Certain acts not permitted**

2 If ASIO could not undertake a particular act in at least one State or
3 Territory without it being authorised by warrant under Division 2
4 of Part III of the *Australian Security Intelligence Organisation Act*
5 *1979* or under Part 2-2 of the *Telecommunications (Interception*
6 *and Access) Act 1979*, this Division does not allow ASIS to
7 undertake the act.

8 **13E Director-General to be satisfied of certain matters**

9 The Director-General must be satisfied that:

- 10 (a) there are satisfactory arrangements in place to ensure that
11 activities will be undertaken in accordance with section 13B
12 only for the specific purpose of supporting ASIO in the
13 performance of its functions; and
14 (b) there are satisfactory arrangements in place to ensure that the
15 nature and consequences of acts done in accordance with
16 section 13B will be reasonable, having regard to the purposes
17 for which they are carried out.

18 **13F Other matters relating to activities undertaken in relation to**
19 **ASIO**

20 *ASIO to be consulted before communicating intelligence*

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

25 *Intelligence to be communicated to ASIO*

- 26 (2) If, in undertaking an activity or series of activities in accordance
27 with section 13B, ASIS produces intelligence, ASIS must cause the
28 intelligence to be communicated to ASIO as soon as practicable
29 after the production.

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

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

7 *Reports about activities to be given to the responsible Minister*

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

12 **13G Guidelines relating to activities undertaken in relation to ASIO**

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

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

19 **12 Before section 14**

20 Insert:

21 **Division 4—Other**

22 **13 Subsection 14(2)**

23 Omit “done inside Australia”, substitute “(whether done inside or
24 outside Australia)”.

25 **14 After subclause 1(1) of Schedule 2**

26 Insert:

27 (1A) The provision to a person of a weapon, or training in the use of a
28 weapon or in self-defence techniques, is not prevented by
29 subsection 6(4) if:

30 (a) the person:

- 1 (i) is an officer of an authority with which ASIS is
2 co-operating in accordance with paragraph 13(1)(c); or
3 (ii) is an officer (however described) of a Commonwealth
4 authority, or a State authority, and is authorised in that
5 capacity to carry and use weapons; and
6 (b) it is provided in accordance with a Ministerial approval under
7 subclause (3A) in relation to the person; and
8 (c) it is provided for the purpose of enabling the person:
9 (i) to protect himself or herself; or
10 (ii) to protect a staff member or agent of ASIS; or
11 (iii) to protect a person who is co-operating with ASIS in
12 accordance with section 13.

13 **15 Subparagraph 1(2)(a)(ii) of Schedule 2**

14 After “(1)”, insert “or (1A)”.

15 **16 After subclause 1(2) of Schedule 2**

16 Insert:

- 17 (2A) The use of a weapon or self-defence techniques is not prevented by
18 subsection 6(4) if:
19 (a) the weapon or techniques are used in the proper performance
20 of a function of ASIS; and
21 (b) the weapon or techniques are used in a controlled
22 environment; and
23 (c) guidelines have been issued by the Director-General under
24 subclause (6); and
25 (d) the weapon or techniques are used in compliance with those
26 guidelines.

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

- 29 (a) the use of a firearm at a rifle range;
30 (b) the use of a martial art at a martial arts club.

31 **17 After subclause 1(3) of Schedule 2**

32 Insert:

- 33 (3A) The Minister may, by written notice given to the Director-General,
34 approve the provision of a weapon, or training in the use of a

1 weapon or in self-defence techniques, to a specified person for the
2 purposes of paragraph (1A)(b).

3 **18 Subclause 1(4) of Schedule 2**

4 After “An approval”, insert “under subclause (3) or (3A)”.

5 **19 Subclause 1(5) of Schedule 2**

6 After “an approval”, insert “under subclause (3) or (3A)”.

7 **20 Clause 2 of Schedule 2**

8 Omit “A staff member or agent of ASIS”, substitute “A person”.

1 **Schedule 6—Protection of information**

2 **Part 1—Main amendments**

3 *Australian Security Intelligence Organisation Act 1979*

4 **1 Subsection 18(2) (penalty)**

5 Omit “2 years”, substitute “10 years”.

6 **2 After subsection 18(2)**

7 Insert:

8 *Exception—information or matter lawfully available*

9 (2A) Subsection (1) does not apply to information or matter that has
10 already been communicated or made available to the public with
11 the authority of the Commonwealth.

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

14 **3 Subsection 18(5)**

15 Repeal the subsection.

16 **4 After section 18**

17 Insert:

18 **18A Unauthorised dealing with records**

19 *Offence for unauthorised dealing with records*

- 20 (1) A person commits an offence if:
- 21 (a) the person is, or has been, an entrusted person; and
 - 22 (b) the person has obtained a record in the person’s capacity as
23 an entrusted person; and
 - 24 (c) the record:
 - 25 (i) was acquired or prepared by or on behalf of the
26 Organisation in connection with its functions; or
 - 27 (ii) relates to the performance by the Organisation of its
28 functions; and

- 1 (d) the person engages in any of the following conduct (the
2 **relevant conduct**):
3 (i) copying the record;
4 (ii) transcribing the record;
5 (iii) retaining the record;
6 (iv) removing the record;
7 (v) dealing with the record in any other manner; and
8 (e) the relevant conduct was not engaged in by the person:
9 (i) as an ASIO employee in the course of the person's
10 duties as an ASIO employee; or
11 (ii) as an ASIO affiliate in accordance with the contract,
12 agreement or other arrangement under which the person
13 is performing functions or services for the Organisation;
14 or
15 (iii) in accordance with a contract, agreement or
16 arrangement the person has entered into with ASIO
17 (other than as an ASIO affiliate); or
18 (iv) acting within the limits of authority conferred on the
19 person by the Director-General; or
20 (v) with the approval of the Director-General, or of a person
21 having the authority of the Director-General to give
22 such an approval.

23 Penalty: Imprisonment for 3 years.

24 *Exception—record lawfully available*

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

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

30 *Alternative verdict*

- 31 (3) Subsection (4) applies if, in a prosecution for an offence (the
32 **prosecuted offence**) against subsection (1), the trier of fact:
33 (a) is not satisfied that the defendant is guilty of the prosecuted
34 offence; but

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

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

8 *Definitions*

9 (5) In this section:

10 ***entrusted person*** means:

- 11 (a) an ASIO employee; or
12 (b) an ASIO affiliate; or
13 (c) a person who has entered into a contract, agreement or
14 arrangement with ASIO (otherwise than as an ASIO
15 affiliate).

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

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

21 ***signals*** includes electromagnetic emissions.

22 **18B Unauthorised recording of information or matter**

- 23 (1) A person commits an offence if:
24 (a) the person is, or has been, an entrusted person; and
25 (b) information or matter has come to the knowledge or into the
26 possession of the person in the person's capacity as an
27 entrusted person; and
28 (c) the information or matter:
29 (i) was acquired or prepared by or on behalf of the
30 Organisation in connection with its functions; or
31 (ii) relates to the performance by the Organisation of its
32 functions; and
33 (d) the person makes a record of the information or matter; and
-

- 1 (e) the record is not made by the person:
2 (i) as an ASIO employee in the course of the person's
3 duties as an ASIO employee; or
4 (ii) as an ASIO affiliate in accordance with the contract,
5 agreement or other arrangement under which the person
6 is performing functions or services for the Organisation;
7 or
8 (iii) in accordance with a contract, agreement or
9 arrangement the person has entered into with ASIO
10 (other than as an ASIO affiliate); or
11 (iv) acting within the limits of authority conferred on the
12 person by the Director-General; or
13 (v) with the approval of the Director-General, or of a person
14 having the authority of the Director-General to give
15 such an approval.

16 Penalty: Imprisonment for 3 years.

17 *Exception—information or matter lawfully available*

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

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

23 *Alternative verdict*

- 24 (3) Subsection (4) applies if, in a prosecution for an offence (the
25 **prosecuted offence**) against subsection (1), the trier of fact:
26 (a) is not satisfied that the defendant is guilty of the prosecuted
27 offence; but
28 (b) is satisfied beyond reasonable doubt that the defendant is
29 guilty of an offence against subsection 18A(1) (the
30 **alternative offence**).
- 31 (4) The trier of fact may find the defendant not guilty of the prosecuted
32 offence but guilty of the alternative offence, so long as the
33 defendant has been accorded procedural fairness in relation to that
34 finding of guilt.

1 *Definitions*

2 (5) In this section:

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

4 *record* has the same meaning as in section 18A.

5 **18C Offences against section 18, 18A or 18B—general rules**

6 *Extended geographical jurisdiction*

7 (1) Section 15.4 of the *Criminal Code* (extended geographical
8 jurisdiction—category D) applies to an offence against section 18,
9 18A or 18B.

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

12 *Institution of prosecution*

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

16 (4) However:

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

20 (b) such a person may be remanded in custody or on bail;
21 even if the consent of the Attorney-General or a person acting
22 under his or her direction has not been obtained, but no further
23 proceedings are to be taken until that consent has been obtained.

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

26 **5 Section 22 (definition of *signals*)**

27 Omit “light emissions and”.

1 ***Intelligence Services Act 2001***

2 **6 Section 3**

3 Insert:

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

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

9 **7 Section 3**

10 Insert:

11 *signals* includes electromagnetic emissions.

12 **8 Before section 39**

13 Insert:

14 **Division 1—Secrecy**

15 **9 Paragraph 39(1)(a)**

16 Before “prepared by”, insert “acquired or”.

17 **10 Subsection 39(1) (penalty)**

18 Repeal the penalty, substitute:

19 Penalty: Imprisonment for 10 years.

20 **11 Subsection 39(2)**

21 Repeal the subsection, substitute:

22 *Exception—information or matter lawfully available*

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

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

1 **12 Paragraph 39A(1)(a)**

2 Before “prepared by”, insert “acquired or”.

3 **13 Subsection 39A(1) (penalty)**

4 Repeal the penalty, substitute:

5 Penalty: Imprisonment for 10 years.

6 **14 Subsection 39A(2)**

7 Repeal the subsection, substitute:

8 *Exception—information or matter lawfully available*

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

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

14 **15 Paragraph 40(1)(a)**

15 Before “prepared by”, insert “acquired or”.

16 **16 Subsection 40(1) (penalty)**

17 Repeal the penalty, substitute:

18 Penalty: Imprisonment for 10 years.

19 **17 Subsection 40(2)**

20 Repeal the subsection, substitute:

21 *Exception—information or matter lawfully available*

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

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

27 **18 After section 40**

28 Insert:

1 **40A Communication of certain information—ONA**

2 (1) A person commits an offence if:

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

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

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

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

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

16 (c) the communication was not made:

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

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

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

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

29 Penalty: Imprisonment for 10 years.

30 *Exception—information or matter lawfully available*

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

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

1 **40B Communication of certain information—DIO**

2 (1) A person commits an offence if:

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

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

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

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

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

16 (c) the communication was not made:

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

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

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

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

28 **Penalty:** Imprisonment for 10 years.

29 *Exception—information or matter lawfully available*

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

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

1 **40C Unauthorised dealing with records—ASIS**

2 (1) A person commits an offence if:

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

5 (i) copying a record;

6 (ii) transcribing a record;

7 (iii) retaining a record;

8 (iv) removing a record;

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

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

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

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

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

18 (c) the record:

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

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

22 (d) the relevant conduct was not engaged in:

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

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

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

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

32 Penalty: Imprisonment for 3 years.

33 *Exception—record lawfully available*

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

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

3 *Alternative verdict*

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

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

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

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

15 **40D Unauthorised recording of information or matter—ASIS**

16 (1) A person commits an offence if:

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

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

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

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

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

27 (c) the information or matter:

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

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

31 (d) the record was not made:

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

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

- 1 (iii) by the person acting within the limits of authority
2 conferred on the person by the Director-General; or
3 (iv) with the approval of the Director-General or of a staff
4 member having the authority of the Director-General to
5 give such an approval.

6 Penalty: Imprisonment for 3 years.

7 *Exception—information or matter lawfully available*

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

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

13 *Alternative verdict*

- 14 (3) Subsection (4) applies if, in a prosecution for an offence (the
15 ***prosecuted offence***) against subsection (1), the trier of fact:
16 (a) is not satisfied that the defendant is guilty of the prosecuted
17 offence; but
18 (b) is satisfied beyond reasonable doubt that the defendant is
19 guilty of an offence against subsection 40C(1) (the
20 ***alternative offence***).
- 21 (4) The trier of fact may find the defendant not guilty of the prosecuted
22 offence but guilty of the alternative offence, so long as the
23 defendant has been accorded procedural fairness in relation to that
24 finding of guilt.

25 **40E Unauthorised dealing with records—AGO**

- 26 (1) A person commits an offence if:
27 (a) the person engages in any of the following conduct (the
28 ***relevant conduct***):
29 (i) copying a record;
30 (ii) transcribing a record;
31 (iii) retaining a record;
32 (iv) removing a record;
33 (v) dealing with a record in any other manner; and
-

- 1 (b) the record was obtained by the person by reason of:
2 (i) his or her being, or having been, a staff member of
3 AGO; or
4 (ii) his or her having entered into any contract, agreement or
5 arrangement with AGO; or
6 (iii) his or her having been an employee or agent of a person
7 who has entered into a contract, agreement or
8 arrangement with AGO; and
9 (c) the record:
10 (i) was acquired or prepared by or on behalf of AGO in
11 connection with its functions; or
12 (ii) relates to the performance by AGO of its functions; and
13 (d) the relevant conduct was not engaged in:
14 (i) in the course of the person's duties as a staff member; or
15 (ii) by the person in accordance with a contract, agreement
16 or arrangement with AGO; or
17 (iii) by the person acting within the limits of authority
18 conferred on the person by the Director of AGO; or
19 (iv) with the approval of the Director of AGO or of a staff
20 member having the authority of the Director of AGO to
21 give such an approval.

22 Penalty: Imprisonment for 3 years.

23 *Exception—record lawfully available*

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

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

29 *Alternative verdict*

30 (3) Subsection (4) applies if, in a prosecution for an offence (the
31 **prosecuted offence**) against subsection (1), the trier of fact:
32 (a) is not satisfied that the defendant is guilty of the prosecuted
33 offence; but

- 1 (b) is satisfied beyond reasonable doubt that the defendant is
2 guilty of an offence against subsection 40F(1) (the
3 *alternative offence*).
- 4 (4) The trier of fact may find the defendant not guilty of the prosecuted
5 offence but guilty of the alternative offence, so long as the
6 defendant has been accorded procedural fairness in relation to that
7 finding of guilt.

8 **40F Unauthorised recording of information or matter—AGO**

- 9 (1) A person commits an offence if:
- 10 (a) the person makes a record of any information or matter; and
11 (b) the information or matter has come to the knowledge or into
12 the possession of the person by reason of:
- 13 (i) his or her being, or having been, a staff member of
14 AGO; or
15 (ii) his or her having entered into any contract, agreement or
16 arrangement with AGO; or
17 (iii) his or her having been an employee or agent of a person
18 who has entered into a contract, agreement or
19 arrangement with AGO; and
- 20 (c) the information or matter:
- 21 (i) was acquired or prepared by or on behalf of AGO in
22 connection with its functions; or
23 (ii) relates to the performance by AGO of its functions; and
- 24 (d) the record was not made:
- 25 (i) in the course of the person's duties as a staff member; or
26 (ii) in accordance with a contract, agreement or
27 arrangement with AGO; or
28 (iii) by the person acting within the limits of authority
29 conferred on the person by the Director of AGO; or
30 (iv) with the approval of the Director of AGO or of a staff
31 member having the authority of the Director of AGO to
32 give such an approval.

33 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*.

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

- 1 (c) the record:
2 (i) was acquired or prepared by or on behalf of ASD in
3 connection with its functions; or
4 (ii) relates to the performance by ASD of its functions; and
5 (d) the relevant conduct was not engaged in:
6 (i) in the course of the person's duties as a staff member; or
7 (ii) in accordance with a contract, agreement or
8 arrangement with ASD; or
9 (iii) by the person acting within the limits of authority
10 conferred on the person by the Director of ASD; or
11 (iv) with the approval of the Director of ASD or of a staff
12 member having the authority of the Director of ASD to
13 give such an approval.

14 Penalty: Imprisonment for 3 years.

15 *Exception—record lawfully available*

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

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

21 *Alternative verdict*

- 22 (3) Subsection (4) applies if, in a prosecution for an offence (the
23 **prosecuted offence**) against subsection (1), the trier of fact:
24 (a) is not satisfied that the defendant is guilty of the prosecuted
25 offence; but
26 (b) is satisfied beyond reasonable doubt that the defendant is
27 guilty of an offence against subsection 40H(1) (the
28 **alternative offence**).
- 29 (4) The trier of fact may find the defendant not guilty of the prosecuted
30 offence but guilty of the alternative offence, so long as the
31 defendant has been accorded procedural fairness in relation to that
32 finding of guilt.

1 **40H Unauthorised recording of information or matter—ASD**

- 2 (1) A person commits an offence if:
- 3 (a) the person makes a record of any information or matter; and
- 4 (b) the information or matter has come to the knowledge or into
- 5 the possession of the person by reason of:
- 6 (i) his or her being, or having been, a staff member of
- 7 ASD; or
- 8 (ii) his or her having entered into any contract, agreement or
- 9 arrangement with ASD; or
- 10 (iii) his or her having been an employee or agent of a person
- 11 who has entered into a contract, agreement or
- 12 arrangement with ASD; and
- 13 (c) the information or matter:
- 14 (i) was acquired or prepared by or on behalf of ASD in
- 15 connection with its functions; or
- 16 (ii) relates to the performance by ASD of its functions; and
- 17 (d) the record was not made:
- 18 (i) in the course of the person's duties as a staff member; or
- 19 (ii) in accordance with a contract, agreement or
- 20 arrangement with ASD; or
- 21 (iii) by the person acting within the limits of authority
- 22 conferred on the person by the Director of ASD; or
- 23 (iv) with the approval of the Director of ASD or of a staff
- 24 member having the authority of the Director of ASD to
- 25 give such an approval.

26 Penalty: Imprisonment for 3 years.

27 *Exception—information or matter lawfully available*

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

31 Note: A defendant bears an evidential burden in relation to the matter in

32 subsection (2): see subsection 13.3(3) of the *Criminal Code*.

33 *Alternative verdict*

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

- 1 (a) is not satisfied that the defendant is guilty of the prosecuted
2 offence; but
3 (b) is satisfied beyond reasonable doubt that the defendant is
4 guilty of an offence against subsection 40G(1) (the
5 *alternative offence*).
- 6 (4) The trier of fact may find the defendant not guilty of the prosecuted
7 offence but guilty of the alternative offence, so long as the
8 defendant has been accorded procedural fairness in relation to that
9 finding of guilt.

10 **40J Unauthorised dealing with records—ONA**

- 11 (1) A person commits an offence if:
12 (a) the person engages in any of the following conduct (the
13 *relevant conduct*):
14 (i) copying a record;
15 (ii) transcribing a record;
16 (iii) retaining a record;
17 (iv) removing a record;
18 (v) dealing with a record in any other manner; and
19 (b) the record was obtained by the person by reason of:
20 (i) his or her being, or having been, a staff member of
21 ONA; or
22 (ii) his or her having entered into any contract, agreement or
23 arrangement with ONA; or
24 (iii) his or her having been an employee or agent of a person
25 who has entered into a contract, agreement or
26 arrangement with ONA; and
27 (c) the record:
28 (i) was acquired or prepared by or on behalf of ONA in
29 connection with its functions; or
30 (ii) relates to the performance by ONA of its functions; and
31 (d) the relevant conduct was not engaged in:
32 (i) in the course of the person's duties as a staff member; or
33 (ii) in accordance with a contract, agreement or
34 arrangement with ONA; or

- 1 (iii) by the person acting within the limits of authority
2 conferred on the person by the Director-General of
3 ONA; or
4 (iv) with the approval of the Director-General of ONA or of
5 a staff member having the authority of the
6 Director-General of ONA to give such an approval.

7 Penalty: Imprisonment for 3 years.

8 *Exception—record lawfully available*

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

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

14 *Alternative verdict*

- 15 (3) Subsection (4) applies if, in a prosecution for an offence (the
16 ***prosecuted offence***) against subsection (1), the trier of fact:
17 (a) is not satisfied that the defendant is guilty of the prosecuted
18 offence; but
19 (b) is satisfied beyond reasonable doubt that the defendant is
20 guilty of an offence against subsection 40K(1) (the
21 ***alternative offence***).
- 22 (4) The trier of fact may find the defendant not guilty of the prosecuted
23 offence but guilty of the alternative offence, so long as the
24 defendant has been accorded procedural fairness in relation to that
25 finding of guilt.

26 **40K Unauthorised recording of information or matter—ONA**

- 27 (1) A person commits an offence if:
28 (a) the person makes a record of any information or matter; and
29 (b) the information or matter has come to the knowledge or into
30 the possession of the person by reason of:
31 (i) his or her being, or having been, a staff member of
32 ONA; or
33 (ii) his or her having entered into any contract, agreement or
34 arrangement with ONA; or
-

- 1 (iii) his or her having been an employee or agent of a person
2 who has entered into a contract, agreement or
3 arrangement with ONA; and
4 (c) the information or matter:
5 (i) was acquired or prepared by or on behalf of ONA in
6 connection with its functions; or
7 (ii) relates to the performance by ONA of its functions; and
8 (d) the record was not made:
9 (i) in the course of the person's duties as a staff member; or
10 (ii) in accordance with a contract, agreement or
11 arrangement with ONA; or
12 (iii) by the person acting within the limits of authority
13 conferred on the person by the Director-General of
14 ONA; or
15 (iv) with the approval of the Director-General of ONA or of
16 a staff member having the authority of the
17 Director-General of ONA to give such an approval.

18 Penalty: Imprisonment for 3 years.

19 *Exception—information or matter lawfully available*

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

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

25 *Alternative verdict*

- 26 (3) Subsection (4) applies if, in a prosecution for an offence (the
27 **prosecuted offence**) against subsection (1), the trier of fact:
28 (a) is not satisfied that the defendant is guilty of the prosecuted
29 offence; but
30 (b) is satisfied beyond reasonable doubt that the defendant is
31 guilty of an offence against subsection 40J(1) (the **alternative**
32 **offence**).
- 33 (4) The trier of fact may find the defendant not guilty of the prosecuted
34 offence but guilty of the alternative offence, so long as the

1 defendant has been accorded procedural fairness in relation to that
2 finding of guilt.

3 **40L Unauthorised dealing with records—DIO**

4 (1) A person commits an offence if:

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

7 (i) copying a record;

8 (ii) transcribing a record;

9 (iii) retaining a record;

10 (iv) removing a record;

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

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

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

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

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

20 (c) the record:

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

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

24 (d) the relevant conduct was not engaged in:

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

26 (ii) in accordance with a contract, agreement or
27 arrangement with DIO; or

28 (iii) by the person acting within the limits of authority
29 conferred on the person by the Director of DIO; or

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

33 Penalty: Imprisonment for 3 years.

1 *Exception—record lawfully available*

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

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

7 *Alternative verdict*

- 8 (3) Subsection (4) applies if, in a prosecution for an offence (the
9 ***prosecuted offence***) against subsection (1), the trier of fact:
10 (a) is not satisfied that the defendant is guilty of the prosecuted
11 offence; but
12 (b) is satisfied beyond reasonable doubt that the defendant is
13 guilty of an offence against subsection 40M(1) (the
14 ***alternative offence***).
- 15 (4) The trier of fact may find the defendant not guilty of the prosecuted
16 offence but guilty of the alternative offence, so long as the
17 defendant has been accorded procedural fairness in relation to that
18 finding of guilt.

19 **40M Unauthorised recording of information or matter—DIO**

- 20 (1) A person commits an offence if:
21 (a) the person makes a record of any information or matter; and
22 (b) the information or matter has come to the knowledge or into
23 the possession of the person by reason of:
24 (i) his or her being, or having been, a staff member of DIO;
25 or
26 (ii) his or her having entered into any contract, agreement or
27 arrangement with DIO; or
28 (iii) his or her having been an employee or agent of a person
29 who has entered into a contract, agreement or
30 arrangement with DIO; and
31 (c) the information or matter:
32 (i) was acquired or prepared by or on behalf of DIO in
33 connection with its functions; or
34 (ii) relates to the performance by DIO of its functions; and
35 (d) the record was not made:
-

- 1 (i) in the course of the person's duties as a staff member; or
2 (ii) in accordance with a contract, agreement or
3 arrangement with DIO; or
4 (iii) by the person acting within the limits of authority
5 conferred on the person by the Director of DIO; or
6 (iv) with the approval of the Director of DIO or of a staff
7 member having the authority of the Director of DIO to
8 give such an approval.

9 Penalty: Imprisonment for 3 years.

10 *Exception—information or matter lawfully available*

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

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

16 *Alternative verdict*

- 17 (3) Subsection (4) applies if, in a prosecution for an offence (the
18 ***prosecuted offence***) against subsection (1), the trier of fact:
19 (a) is not satisfied that the defendant is guilty of the prosecuted
20 offence; but
21 (b) is satisfied beyond reasonable doubt that the defendant is
22 guilty of an offence against subsection 40L(1) (the
23 ***alternative offence***).
- 24 (4) The trier of fact may find the defendant not guilty of the prosecuted
25 offence but guilty of the alternative offence, so long as the
26 defendant has been accorded procedural fairness in relation to that
27 finding of guilt.

28 **19 Subsection 41(1)**

29 Omit "(1)".

30 **20 Subsection 41(2)**

31 Repeal the subsection.

1 **21 After section 41**

2 Insert:

3 **41A Offences against this Division—general rules**

4 *Extended geographical jurisdiction*

5 (1) Section 15.4 of the *Criminal Code* (extended geographical
6 jurisdiction—category D) applies to an offence against this
7 Division.

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

10 *Institution of prosecution*

11 (3) A prosecution under this Division may be instituted only by, or
12 with the consent of, the Attorney-General or a person acting under
13 the Attorney-General's direction.

14 (4) However:

15 (a) a person charged with an offence against this Division may
16 be arrested, or a warrant for his or her arrest may be issued
17 and executed; and

18 (b) such a person may be remanded in custody or on bail;
19 even if the consent of the Attorney-General or a person acting
20 under his or her direction has not been obtained, but no further
21 proceedings are to be taken until that consent has been obtained.

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

24 **22 Before section 42**

25 Insert:

1 **Division 2—Other matters**

2 **23 Application of amendments**

3 The amendments made by this Part apply in relation to conduct engaged
4 in by a person in relation to records, information or matter after the
5 commencement of this Part, whether the records were obtained, or the
6 information or matter came to the knowledge or into the possession of
7 the person, before or after that commencement.

1 **Part 2—Consequential amendments**

2 *Australian Crime Commission Act 2002*

3 **24 Schedule 1**

4 After “sections 18,” insert “18A, 18B.”

5 *Crimes Act 1914*

6 **25 Subsection 15LC(4) (note 2)**

7 Omit “section 39 or 41”, substitute “under Division 1 of Part 6”.

8 *Privacy Act 1988*

9 **26 Subsection 80P(7) (paragraph (a) of the definition of**
10 ***designated secrecy provision*)**

11 After “sections 18”, insert “, 18A, 18B”.

12 **27 Subsection 80P(7) (paragraph (c) of the definition of**
13 ***designated secrecy provision*)**

14 Repeal the paragraph, substitute:

15 (c) sections 39, 39A, 40, 40A to 40M and 41 of the *Intelligence*
16 *Services Act 2001*;

1 **Schedule 7—Renaming of Defence agencies**

2 **Part 1—Main amendments**

3 *Intelligence Services Act 2001*

4 **1 Section 3 (definition of agency)**

5 Omit “DIGO or DSD”, substitute “AGO or ASD”.

6 **2 Section 3 (paragraphs (aa) and (b) of the definition of**
7 **agency head)**

8 Repeal the paragraphs, substitute:

9 (b) in relation to AGO—the Director of AGO; and

10 (c) in relation to ASD—the Director of ASD.

11 **3 Section 3**

12 Insert:

13 *AGO* means that part of the Defence Department known as the
14 Australian Geospatial-Intelligence Organisation.

15 *ASD* means that part of the Defence Department known as the
16 Australian Signals Directorate.

17 **4 Section 3 (definition of DIGO)**

18 Repeal the definition.

19 **5 Section 3 (definition of DSD)**

20 Repeal the definition.

21 **6 Section 3 (paragraph (a) of the definition of *incidentally***
22 ***obtained intelligence*)**

23 Omit “DIGO”, substitute “AGO”.

24 **7 Section 3 (paragraph (a) of the definition of *incidentally***
25 ***obtained intelligence*)**

26 Omit “DSD”, substitute “ASD”.

1 **8 Section 3 (paragraph (b) of the definition of *intelligence***
2 ***information*)**

3 Omit “DIGO”, substitute “AGO”.

4 **9 Section 3 (paragraph (c) of the definition of *intelligence***
5 ***information*)**

6 Omit “DSD”, substitute “ASD”.

7 **10 Section 6B (heading)**

8 Repeal the heading, substitute:

9 **6B Functions of AGO**

10 **11 Section 6B**

11 Omit “DIGO”, substitute “AGO”.

12 **12 Section 7 (heading)**

13 Repeal the heading, substitute:

14 **7 Functions of ASD**

15 **13 Section 7**

16 Omit “DSD”, substitute “ASD”.

17 **14 Subsection 8(1)**

18 Omit “DIGO”, substitute “AGO”.

19 **15 Subsection 8(1)**

20 Omit “DSD”, substitute “ASD”.

21 **16 Paragraph 11(2)(e)**

22 Omit “DIGO”, substitute “AGO”.

23 **17 Paragraph 11(2)(f)**

24 Omit “DSD”, substitute “ASD”.

1 **18 Section 12A**

2 Omit “Director of DIGO, the Director of DSD”, substitute “Director of
3 AGO, the Director of ASD”.

4 **19 Subsection 14(3) (definition of *staff member*)**

5 Omit “Director of DIGO, the Director of DSD”, substitute “Director of
6 AGO, the Director of ASD”.

7 **20 Subsection 15(1)**

8 Omit “responsible Minister in relation to DIGO and the responsible
9 Minister in relation to DSD”, substitute “responsible Minister in relation
10 to AGO and the responsible Minister in relation to ASD”.

11 **21 Paragraph 15(3)(ab)**

12 Omit “DIGO” (wherever occurring), substitute “AGO”.

13 **22 Paragraph 15(3)(b)**

14 Omit “DSD” (wherever occurring), substitute “ASD”.

15 **23 Paragraph 29(1)(a)**

16 Omit “DIGO” (first occurring), substitute “AGO”.

17 **24 Paragraph 29(1)(a)**

18 Omit “DSD” (first occurring), substitute “ASD”.

19 **25 Paragraph 29(1)(a)**

20 Omit “DIGO” (second occurring), substitute “AGO”.

21 **26 Paragraph 29(1)(a)**

22 Omit “DSD” (second occurring), substitute “ASD”.

23 **27 Paragraph 29(1)(b)**

24 Omit “DIGO”, substitute “AGO”.

25 **28 Paragraph 29(1)(b)**

26 Omit “DSD”, substitute “ASD”.

- 1 **29 Subsection 29(2)**
2 Omit “DIGO”, substitute “AGO”.
- 3 **30 Subsection 29(2)**
4 Omit “DSD”, substitute “ASD”.
- 5 **31 Paragraph 29(3)(a)**
6 Omit “DIGO”, substitute “AGO”.
- 7 **32 Paragraph 29(3)(a)**
8 Omit “DSD”, substitute “ASD”.
- 9 **33 Paragraph 29(3)(b)**
10 Omit “DIGO”, substitute “AGO”.
- 11 **34 Paragraph 29(3)(b)**
12 Omit “DSD”, substitute “ASD”.
- 13 **35 Paragraph 29(3)(c)**
14 Omit “DIGO”, substitute “AGO”.
- 15 **36 Paragraph 29(3)(c)**
16 Omit “DSD”, substitute “ASD”.
- 17 **37 Paragraph 29(3)(e)**
18 Omit “DIGO”, substitute “AGO”.
- 19 **38 Paragraph 29(3)(e)**
20 Omit “DSD”, substitute “ASD”.
- 21 **39 Paragraph 29(3)(g)**
22 Omit “DIGO”, substitute “AGO”.
- 23 **40 Paragraph 29(3)(g)**
24 Omit “DSD”, substitute “ASD”.
- 25 **41 Paragraph 30(baa)**
26 Omit “DIGO”, substitute “AGO”.
-

1 **42 Paragraph 30(ba)**

2 Omit “DSD”, substitute “ASD”.

3 **43 Section 39A (heading)**

4 Repeal the heading, substitute:

5 **39A Communication of certain information—AGO**

6 **44 Subsection 39A(1)**

7 Omit “DIGO” (wherever occurring), substitute “AGO”.

8 **45 Section 40 (heading)**

9 Repeal the heading, substitute:

10 **40 Communication of certain information—ASD**

11 **46 Subsection 40(1)**

12 Omit “DSD” (wherever occurring), substitute “ASD”.

13 **47 Clause 1A of Schedule 1 (definition of *agency*)**

14 Omit “DIGO”, substitute “AGO”.

15 **48 Clause 1A of Schedule 1 (definition of *agency*)**

16 Omit “DSD”, substitute “ASD”.

17 **49 Clause 1A of Schedule 1 (paragraph (ba) of the definition**
18 **of *agency head*)**

19 Omit “DIGO”, substitute “AGO”.

20 **50 Clause 1A of Schedule 1 (paragraph (c) of the definition of**
21 ***agency head*)**

22 Omit “DSD”, substitute “ASD”.

23 **51 Clause 1A of Schedule 1 (paragraph (a) of the definition of**
24 ***operationally sensitive information*)**

25 Omit “DIGO”, substitute “AGO”.

1 **52 Clause 1A of Schedule 1 (paragraph (a) of the definition of**
2 ***operationally sensitive information*)**

3 Omit “DSD”, substitute “ASD”.

4 **53 Clause 1A of Schedule 1 (paragraph (b) of the definition of**
5 ***operationally sensitive information*)**

6 Omit “DIGO”, substitute “AGO”.

7 **54 Clause 1A of Schedule 1 (paragraph (b) of the definition of**
8 ***operationally sensitive information*)**

9 Omit “DSD”, substitute “ASD”.

10 **55 Paragraph 7(1)(a) of Schedule 1**

11 Omit “DIGO or DSD”, substitute “AGO or ASD”.

12 **56 Paragraph 20(2)(c) of Schedule 1**

13 Omit “DIGO”, substitute “AGO”.

14 **57 Paragraph 20(2)(c) of Schedule 1**

15 Omit “DSD”, substitute “ASD”.

1 **Part 2—Consequential amendments**

2 ***Anti-Money Laundering and Counter-Terrorism Financing***
3 ***Act 2006***

4 **58 Section 5**

5 Insert:

6 *AGO* means that part of the Defence Department known as the
7 Australian Geospatial-Intelligence Organisation, and includes any
8 part of the Defence Force that performs functions on behalf of that
9 part of the Department.

10 *ASD* means that part of the Defence Department known as the
11 Australian Signals Directorate, and includes any part of the
12 Defence Force that performs functions on behalf of that part of the
13 Department.

14 **59 Section 5 (definition of *defence intelligence agency*)**

15 Omit “DIGO”, substitute “AGO”.

16 **60 Section 5 (definition of *defence intelligence agency*)**

17 Omit “DSD”, substitute “ASD”.

18 **61 Section 5 (paragraph (gb) of the definition of *designated***
19 ***agency*)**

20 Repeal the paragraph, substitute:
21 (gb) AGO; or

22 **62 Section 5 (paragraph (gd) of the definition of *designated***
23 ***agency*)**

24 Repeal the paragraph, substitute:
25 (gd) ASD; or

26 **63 Section 5 (definition of *DIGO*)**

27 Repeal the definition.

1 **64 Section 5 (definition of *DIO*)**

2 Omit “Department of Defence”, substitute “Defence Department”.

3 **65 Section 5 (definition of *DSD*)**

4 Repeal the definition.

5 **66 Paragraph 128(13B)(d)**

6 Omit “DIGO or DSD” (wherever occurring), substitute “AGO or ASD”.

7 ***Archives Act 1983***

8 **67 Paragraphs 29(8)(ba) and (c)**

9 Repeal the paragraphs, substitute:

10 (ba) the Australian Geospatial-Intelligence Organisation;

11 (c) the Australian Signals Directorate;

12 ***Australian Human Rights Commission Act 1986***

13 **68 Subsection 11(4)**

14 Omit “Defence Signals Directorate”, substitute “Australian Signals
15 Directorate”.

16 **69 Subsection 11(4)**

17 Omit “Defence Imagery and Geospatial Organisation”, substitute
18 “Australian Geospatial-Intelligence Organisation”.

19 **70 Subsection 21(3)**

20 Omit “Defence Imagery and Geospatial Organisation”, substitute
21 “Australian Geospatial-Intelligence Organisation”.

22 **71 Subsection 21(3)**

23 Omit “Defence Signals Directorate”, substitute “Australian Signals
24 Directorate”.

1 ***Australian Security Intelligence Organisation Act 1979***

2 **72 Section 4**

3 Insert:

4 *AGO* has the meaning given by the *Intelligence Services Act 2001*.

5 *ASD* has the meaning given by the *Intelligence Services Act 2001*.

6 **73 Section 4 (definition of DIGO)**

7 Repeal the definition.

8 **74 Section 4 (definition of DSD)**

9 Repeal the definition.

10 **75 Section 4 (paragraph (c) of the definition of *intelligence or***
11 ***security agency*)**

12 Omit “Defence Imagery and Geospatial Organisation”, substitute
13 “Australian Geospatial-Intelligence Organisation”.

14 **76 Section 4 (paragraph (e) of the definition of *intelligence or***
15 ***security agency*)**

16 Omit “Defence Signals Directorate”, substitute “Australian Signals
17 Directorate”.

18 **77 Subsection 18(4A) (heading)**

19 Repeal the heading, substitute:

20 *Communicating information to ASIS, ASD and AGO*

21 **78 Subsection 18(4A)**

22 Omit “DSD or DIGO”, substitute “ASD or AGO”.

23 **79 Paragraph 18(4A)(b)**

24 Omit “DSD or DIGO’s”, substitute “ASD or AGO’s”.

25 **80 Paragraphs 19A(1)(b) and (c)**

26 Repeal the paragraphs, substitute:

27 (b) ASD;

1 (c) AGO;

2 **81 Subsection 19A(4) (note 1)**

3 Omit “DSD and DIGO”, substitute “ASD and AGO”.

4 **82 Subsection 35(1) (paragraph (d) of the definition of *agency***
5 ***head*)**

6 Omit “Defence Imagery and Geospatial Organisation”, substitute
7 “Australian Geospatial-Intelligence Organisation”.

8 **83 Subsection 35(1) (paragraph (f) of the definition of *agency***
9 ***head*)**

10 Omit “Defence Signals Directorate”, substitute “Australian Signals
11 Directorate”.

12 ***Crimes Act 1914***

13 **84 Paragraph 15KY(3)(b)**

14 Omit “Defence Signals Directorate”, substitute “Australian Signals
15 Directorate”.

16 **85 Paragraph 15KY(3)(c)**

17 Omit “Defence Imagery and Geospatial Organisation”, substitute
18 “Australian Geospatial-Intelligence Organisation”.

19 **86 Section 85ZL (paragraph (d) of the definition of**
20 ***intelligence or security agency*)**

21 Omit “Defence Signals Directorate”, substitute “Australian Signals
22 Directorate”.

23 **87 Section 85ZL (paragraph (f) of the definition of *intelligence***
24 ***or security agency*)**

25 Omit “Defence Imagery and Geospatial Organisation”, substitute
26 “Australian Geospatial-Intelligence Organisation”.

1 ***Crimes (Overseas) Act 1964***

2 **88 Section 3**

3 Insert:

4 *AGO* has the same meaning as in the *Intelligence Services Act*
5 *2001*.

6 *ASD* has the same meaning as in the *Intelligence Services Act*
7 *2001*.

8 **89 Section 3 (definition of *DIGO*)**

9 Repeal the definition.

10 **90 Section 3 (definition of *DSD*)**

11 Repeal the definition.

12 **91 Section 3 (definition of *staff member*)**

13 Omit “*DIGO* or *DSD*”, substitute “*AGO* or *ASD*”.

14 **92 Subsection 3A(10) (heading)**

15 Repeal the heading, substitute:

16 *Defence Force members and ASIS, AGO and ASD staff not covered*

17 **93 Paragraph 3A(10)(b)**

18 Omit “*DIGO* or *DSD*” (wherever occurring), substitute “*AGO* or *ASD*”.

19 **94 Subsection 3A(10) (paragraph (a) of the note)**

20 Omit “*DIGO* or *DSD*”, substitute “*AGO* or *ASD*”.

21 ***Criminal Code Act 1995***

22 **95 Section 473.1 of the *Criminal Code* (paragraph (d) of the**
23 **definition of *intelligence or security officer*)**

24 Omit “Defence Signals Directorate”, substitute “Australian Signals
25 Directorate”.

1 **96 Section 473.1 of the *Criminal Code* (definition of**
2 ***intelligence or security officer*)**

3 Omit “or the Defence Signals Directorate”, substitute “or the Australian
4 Signals Directorate”.

5 **97 Subsection 476.5(1) of the *Criminal Code***

6 Omit “DIGO or DSD”, substitute “AGO or ASD”.

7 **98 Subsection 476.5(3) of the *Criminal Code***

8 Insert:

9 *AGO* means that part of the Defence Department known as the
10 Australian Geospatial-Intelligence Organisation.

11 *ASD* means that part of the Defence Department known as the
12 Australian Signals Directorate.

13 **99 Subsection 476.5(3) of the *Criminal Code* (definition of**
14 ***DIGO*)**

15 Repeal the definition.

16 **100 Subsection 476.5(3) of the *Criminal Code* (definition of**
17 ***DSD*)**

18 Repeal the definition.

19 **101 Subsection 476.5(3) of the *Criminal Code* (paragraph (b)**
20 **of the definition of *staff member*)**

21 Omit “DSD” (wherever occurring), substitute “ASD”.

22 **102 Subsection 476.5(3) of the *Criminal Code* (paragraph (c)**
23 **of the definition of *staff member*)**

24 Omit “DIGO” (wherever occurring), substitute “AGO”.

25 ***Freedom of Information Act 1982***

26 **103 Subsection 4(1)**

27 Insert:

1 ***Australian Geospatial-Intelligence Organisation*** means that part
2 of the Department of Defence known as the Australian
3 Geospatial-Intelligence Organisation.

4 ***Australian Signals Directorate*** means that part of the Department
5 of Defence known as the Australian Signals Directorate.

6 **104 Subsection 4(1) (definition of *Defence Imagery and***
7 ***Geospatial Organisation*)**

8 Repeal the definition.

9 **105 Subsection 4(1) (definition of *Defence Signals***
10 ***Directorate*)**

11 Repeal the definition.

12 **106 Subparagraph 7(2A)(a)(v)**

13 Repeal the subparagraph, substitute:

14 (v) the Australian Geospatial-Intelligence Organisation;

15 **107 Subparagraph 7(2A)(a)(vii)**

16 Repeal the subparagraph, substitute:

17 (vii) the Australian Signals Directorate;

18 **108 Division 2 of Part I of Schedule 2**

19 Insert:

Australian Geospatial-Intelligence Organisation

Australian Signals Directorate

20 **109 Division 2 of Part I of Schedule 2**

21 Omit:

Defence Imagery and Geospatial Organisation

22 **110 Division 2 of Part I of Schedule 2**

23 Omit:

Defence Signals Directorate

1 ***Independent National Security Legislation Monitor Act 2010***

2 **111 Section 4 (paragraph (f) of the definition of *head*)**

3 Omit “Defence Imagery and Geospatial Organisation”, substitute
4 “Australian Geospatial-Intelligence Organisation”.

5 **112 Section 4 (paragraph (h) of the definition of *head*)**

6 Omit “Defence Signals Directorate”, substitute “Australian Signals
7 Directorate”.

8 **113 Section 4 (paragraph (g) of the definition of *law*
9 *enforcement or security agency*)**

10 Omit “Defence Imagery and Geospatial Organisation”, substitute
11 “Australian Geospatial-Intelligence Organisation”.

12 **114 Section 4 (paragraph (i) of the definition of *law*
13 *enforcement or security agency*)**

14 Omit “Defence Signals Directorate”, substitute “Australian Signals
15 Directorate”.

16 ***Inspector-General of Intelligence and Security Act 1986***

17 **115 Subsection 3(1)**

18 Insert:

19 *AGO* means that part of the Defence Department known as the
20 Australian Geospatial-Intelligence Organisation, and any part of
21 the Defence Force that performs functions on behalf of that part of
22 the Department.

23 *ASD* means that part of the Defence Department known as the
24 Australian Signals Directorate, and includes any part of the
25 Defence Force that performs functions on behalf of that part of that
26 Department.

27 **116 Subsection 3(1) (definition of *DIGO*)**

28 Repeal the definition.

- 1 **117 Subsection 3(1) (definition of *DSD*)**
2 Repeal the definition.
- 3 **118 Subsection 3(1) (paragraph (c) of the definition of *head*)**
4 Repeal the paragraph, substitute:
5 (c) in relation to AGO—the Director of AGO; or
- 6 **119 Subsection 3(1) (paragraph (e) of the definition of *head*)**
7 Repeal the paragraph, substitute:
8 (e) in relation to ASD—the Director of ASD; or
- 9 **120 Subsection 3(1) (definition of *intelligence agency*)**
10 Omit “DIGO”, substitute “AGO”.
- 11 **121 Subsection 3(1) (definition of *intelligence agency*)**
12 Omit “DSD”, substitute “ASD”.
- 13 **122 Subsections 8(2) and (4)**
14 Omit “DIGO or DSD”, substitute “AGO or ASD”.
- 15 **123 Subsection 8(5)**
16 Omit “DIGO, DSD”, substitute “AGO, ASD”.
- 17 **124 Paragraph 8A(4)(a)**
18 Omit “DIGO or DSD”, substitute “AGO or ASD”.
- 19 **125 Paragraph 15(3)(b)**
20 Omit “DIGO”, substitute “AGO”.
- 21 **126 Paragraph 15(3)(b)**
22 Omit “DSD”, substitute “ASD”.
- 23 **127 Paragraph 21(1B)(b)**
24 Omit “DIGO”, substitute “AGO”.
- 25 **128 Paragraph 21(1B)(b)**
26 Omit “DSD”, substitute “ASD”.
-

1 **129 Paragraph 32A(1)(d)**

2 Omit “DIGO”, substitute “AGO”.

3 **130 Paragraph 32A(1)(d)**

4 Omit “DSD”, substitute “ASD”.

5 **131 Paragraph 32A(5)(b)**

6 Omit “DIGO”, substitute “AGO”.

7 **132 Paragraph 32A(5)(b)**

8 Omit “DSD”, substitute “ASD”.

9 **133 Subsection 32B(1)**

10 Omit “DIGO or DSD”, substitute “AGO or ASD”.

11 **134 Subsection 35(2B)**

12 Omit “and DSD”, substitute “, AGO and ASD”.

13 ***Privacy Act 1988***

14 **135 Paragraph 7(1)(g)**

15 Omit “Defence Imagery and Geospatial Organisation or the Defence
16 Signals Directorate”, substitute “Australian Geospatial-Intelligence
17 Organisation or the Australian Signals Directorate”.

18 **136 Paragraph 7(1A)(c)**

19 Omit “Defence Signals Directorate”, substitute “Australian Signals
20 Directorate”.

21 **137 Paragraph 7(2)(b)**

22 Omit “Defence Imagery and Geospatial Organisation or the Defence
23 Signals Directorate”, substitute “Australian Geospatial-Intelligence
24 Organisation or the Australian Signals Directorate”.

1 ***Public Interest Disclosure Act 2013***

2 **138 Section 8 (paragraph (c) of the definition of *intelligence***
3 ***agency*)**

4 Omit “Defence Imagery and Geospatial Organisation”, substitute
5 “Australian Geospatial-Intelligence Organisation”.

6 **139 Section 8 (paragraph (e) of the definition of *intelligence***
7 ***agency*)**

8 Omit “Defence Signals Directorate”, substitute “Australian Signals
9 Directorate”.

10 **140 Paragraph 72(1)(g)**

11 Omit “Defence Imagery and Geospatial Organisation”, substitute
12 “Australian Geospatial-Intelligence Organisation”.

13 **141 Paragraph 72(1)(i)**

14 Omit “Defence Signals Directorate”, substitute “Australian Signals
15 Directorate”.

16 **142 Paragraph 72(4)(a)**

17 Omit “Defence Imagery and Geospatial Organisation”, substitute
18 “Australian Geospatial-Intelligence Organisation”.

19 **143 Paragraph 72(4)(c)**

20 Omit “Defence Signals Directorate”, substitute “Australian Signals
21 Directorate”.

1 **Part 3—Transitional provisions**

2 **144 Transitional—subsection 25B(1) of the Acts**
3 ***Interpretation Act 1901***

4 Subsection 25B(1) of the *Acts Interpretation Act 1901* applies as if:

- 5 (a) that part of the Defence Department known as the Defence
6 Imagery and Geospatial Organisation were a body and the
7 amendments made by Part 1 of this Schedule altered the
8 name of that body to the Australian Geospatial-Intelligence
9 Organisation; and
10 (b) that part of the Defence Department known as the Defence
11 Signals Directorate were a body and the amendments made
12 by Part 1 of this Schedule altered the name of that body to the
13 Australian Signals Directorate.

14 **145 Transitional rules**

15 The Minister may, by legislative instrument, make rules in relation to
16 transitional matters arising out of the amendments and repeals made by
17 Parts 1 and 2 of this Schedule.