SCHEDULE OF THE AMENDMENTS MADE BY THE HOUSE OF REPRESENTATIVES

(1) Clause 2, page 2 (table item 2), omit the table item, substitute:

2. Schedule 1, The day after this Act receives the Royal Part 1 Assent. [commencement]

(2) Schedule 1, page 4 (before line 7), before the heading, insert:

_Australian Security Intelligence Organisation Act 1979_

_1A After subsection 94(2B)_

Insert:

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

(a) the total number of technical assistance requests given by the Director-General under paragraph 317G(1)(a) of the _Telecommunications Act 1997_ during the period; and

(b) the total number of technical assistance notices given by the Director-General under section 317L of the _Telecommunications Act 1997_ during the period; and

(c) the total number of technical capability notices given by the Attorney-General under section 317T of the _Telecommunications Act 1997_ during the period that relate to the Organisation.

(2BB) For the purposes of paragraph (2BA)(c), a technical capability notice relates to the Organisation if the acts or things specified in the notice:

(a) are directed towards ensuring that a designated communications provider (within the meaning of Part 15 of the _Telecommunications Act 1997_) is capable of giving listed help (within the meaning of section 317T of that Act) to the
Organisation in relation to a matter covered by paragraph 317T(2)(a) of that Act; or
(b) are by way of giving help to the Organisation in relation to a matter covered by paragraph 317T(2)(b) of the

[annual report]

(3) Schedule 1, page 4 (after line 27), after item 4, insert:

Independent National Security Legislation Monitor Act 2010

4A At the end of subsection 6(1)
Add:
; (e) the function conferred by subsection (1D).

4B Before subsection 6(2)
Insert:
(1D) The Independent National Security Legislation Monitor must:
(a) review the operation, effectiveness and implications of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018; and
(b) do so as soon as practicable after the 18-month period beginning on the day that Act receives the Royal Assent.

[review]

(4) Schedule 1, item 7, page 5 (line 12) to page 7 (line 8), omit section 317A, substitute:

317A Simplified outline of this Part

- The Director-General of Security, the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Signals Directorate or the chief officer of an interception agency may give a technical assistance request to a designated communications provider.

- A technical assistance request may ask the provider to do acts or things on a voluntary basis that are directed towards ensuring that the provider is capable of giving certain types of help to ASIO, the Australian Secret Intelligence Service, the Australian Signals Directorate or an interception agency in relation to:
  (a) in the case of ASIO—safeguarding national security; or
(b) in the case of the Australian Secret Intelligence Service—the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being; or

(c) in the case of the Australian Signals Directorate—providing material, advice and other assistance on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; or

(d) in the case of an interception agency—enforcing the criminal law, so far as it relates to serious Australian offences; or

(e) in the case of an interception agency—assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences.

• A technical assistance request may ask the provider to give help to ASIO, the Australian Secret Intelligence Service, the Australian Signals Directorate or an interception agency on a voluntary basis in relation to:

(a) in the case of ASIO—safeguarding national security; or

(b) in the case of the Australian Secret Intelligence Service—the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being; or

(c) in the case of the Australian Signals Directorate—providing material, advice and other assistance on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; or

(d) in the case of an interception agency—enforcing the criminal law, so far as it relates to serious Australian offences; or

(e) in the case of an interception agency—assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences.

• The Director-General of Security or the chief officer of an interception agency may give a designated communications provider a notice, to be known as a technical assistance notice, that requires the provider to do acts or things by way of giving certain types of help to ASIO or the agency in relation to:

(a) enforcing the criminal law, so far as it relates to serious Australian offences; or
(b) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or
(c) safeguarding national security.

The Attorney-General may give a designated communications provider a notice, to be known as a technical capability notice.

A technical capability notice may require the provider to do acts or things directed towards ensuring that the provider is capable of giving certain types of help to ASIO or an interception agency in relation to:
(a) enforcing the criminal law, so far as it relates to serious Australian offences; or
(b) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or
(c) safeguarding national security.

A technical capability notice may require the provider to do acts or things by way of giving certain types of help to ASIO or an interception agency in relation to:
(a) enforcing the criminal law, so far as it relates to serious Australian offences; or
(b) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or
(c) safeguarding national security.

[...simplified outline...]

(5) Schedule 1, item 7, page 7 (lines 27 to 29), omit the definition of Corruption and Crime Commission (WA) in section 317B.

[Corruption and Crime Commission (WA)]

(6) Schedule 1, item 7, page 7 (after line 31), after the definition of designated communications provider in section 317B, insert:

electronic protection includes:
(a) authentication; and
(b) encryption.

[electronic protection]
(7) Schedule 1, item 7, page 8 (after line 32), after the definition of giving help in section 317B, insert:

    Home Affairs Minister means the Minister administering the Telecommunications (Interception and Access) Act 1979.

    [Home Affairs Minister]

(8) Schedule 1, item 7, page 9 (lines 1 to 4), omit the definition of Independent Broad-based Anti-corruption Commission of Victoria in section 317B.

    [Independent Broad-based Anti-corruption Commission of Victoria]

(9) Schedule 1, item 7, page 9 (lines 5 to 7), omit the definition of Independent Commissioner Against Corruption (SA) in section 317B.

    [Independent Commissioner Against Corruption (SA)]

(10) Schedule 1, item 7, page 9 (lines 8 to 23), omit the definition of interception agency in section 317B, substitute:

    interception agency means:
    (a) the Australian Federal Police; or
    (b) the Australian Crime Commission; or
    (c) the Police Force of a State or the Northern Territory.

    [interception agency]

(11) Schedule 1, item 7, page 9 (lines 24 to 26), omit the definition of Law Enforcement Conduct Commission of New South Wales in section 317B.

    [Law Enforcement Conduct Commission of New South Wales]

(12) Schedule 1, item 7, page 10 (lines 2 to 5), omit the definition of member of the staff of the Independent Commissioner Against Corruption (SA) in section 317B.

    [member of the staff of the Independent Commissioner Against Corruption (SA)]

(13) Schedule 1, item 7, page 10 (after line 7), after the definition of officer in section 317B, insert:

    Ombudsman official means:
    (a) the Commonwealth Ombudsman; or
    (b) a Deputy Commonwealth Ombudsman; or
    (c) a person who is a member of the staff referred to in subsection 31(1) of the Ombudsman Act 1976.

    [Ombudsman official]
(14) Schedule 1, item 7, page 10 (before line 8), before the definition of staff member in section 317B, insert:

serious Australian offence means an offence against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of 3 years or more for life.

serious foreign offence means an offence against a law in force in a foreign country that is punishable by a maximum term of imprisonment of 3 years or more for life.

[serious offences]

(15) Schedule 1, item 7, page 10 (after line 10), after the definition of staff member in section 317B, insert:

State or Territory inspecting authority, in relation to an interception agency of a State or Territory, means the authority that, under the law of the State or Territory concerned, has the function of making inspections of a similar kind to those provided for in section 55 of the Surveillance Devices Act 2004 when the interception agency is exercising powers under the law of that State or Territory that is of a similar nature to that Act.

[State or Territory inspecting authority]

(16) Schedule 1, item 7, page 10 (after line 19), after the definition of supply in section 317B, insert:

systemic vulnerability means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

systemic weakness means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

[systemic vulnerability and systemic weakness]

(17) Schedule 1, item 7, page 10 (before line 20), before the definition of technical assistance notice in section 317B, insert:

target technology:

(a) for the purposes of this Part, a particular carriage service, so far as the service is used, or is likely to be used, (whether directly or
indirectly) by a particular person, is a target technology that is connected with that person; and

(b) for the purposes of this Part, a particular electronic service, so far as the service is used, or is likely to be used, (whether directly or indirectly) by a particular person, is a target technology that is connected with that person; and

(c) for the purposes of this Part, particular software installed, or to be installed, on:
   (i) a particular computer; or
   (ii) a particular item of equipment;
used, or likely to be used, (whether directly or indirectly) by a particular person is a target technology that is connected with that person; and

(d) for the purposes of this Part, a particular update of software that has been installed on:
   (i) a particular computer; or
   (ii) a particular item of equipment;
used, or likely to be used, (whether directly or indirectly) by a particular person is a target technology that is connected with that person; and

(e) for the purposes of this Part, a particular item of customer equipment used, or likely to be used, (whether directly or indirectly) by a particular person is a target technology that is connected with that person; and

(f) for the purposes of this Part, a particular data processing device used, or likely to be used, (whether directly or indirectly) by a particular person is a target technology that is connected with that person.

For the purposes of paragraphs (a), (b), (c), (d), (e) and (f), it is immaterial whether the person can be identified.

[Target technology]

(18) Schedule 1, item 7, page 10 (after line 24), after subparagraph (a)(i) of the definition of technical assistance notice information in section 317B, insert:
   (ia) consultation relating to the giving of a technical assistance notice;

[Technical assistance notice information]

(19) Schedule 1, item 7, page 11 (after line 22), after subparagraph (a)(iv) of the definition of technical capability notice information in section 317B, insert:
   (iva) consultation relating to the variation of a technical capability notice;

[Technical capability notice information]
(20) Schedule 1, item 7, page 15 (after line 30), after paragraph 317E(1)(d), insert:

(da) an act or thing done to assist in, or facilitate:
   (i) giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or
   (ii) the effective receipt of information in connection with a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

   [listed acts or things]

(21) Schedule 1, item 7, page 16 (lines 34 and 35), omit “and laws imposing pecuniary penalties”, substitute “, so far as it relates to serious Australian offences”.

   [serious offences]

(22) Schedule 1, item 7, page 16 (line 37), after “country”, insert “, so far as those laws relate to serious foreign offences”.

   [serious offences]

(23) Schedule 1, item 7, page 19 (lines 12 to 20), omit subsection 317G(5), substitute:

   Relevant objective

(5) For the purposes of this section, relevant objective means:
   (a) in relation to a technical assistance request given by the Director-General of Security—safeguarding national security; or
   (b) in relation to a technical assistance request given by the Director-General of the Australian Secret Intelligence Service—the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being; or
   (c) in relation to a technical assistance request given by the Director-General of the Australian Signals Directorate—providing material, advice and other assistance to a person or body mentioned in subsection 7(2) of the Intelligence Services Act 2001 on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; or
   (d) in relation to a technical assistance request given by the chief officer of an interception agency:
      (i) enforcing the criminal law, so far as it relates to serious Australian offences; or
(ii) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences.

[technical assistance request—relevant objective]

(24) Schedule 1, item 7, page 20 (after line 34), at the end of section 317H, add:

(5) If, under subsection (3):
   (a) the Director-General of Security; or
   (b) the Director-General of the Australian Secret Intelligence Service; or
   (c) the Director-General of the Australian Signals Directorate; or
   (d) the chief officer of an interception agency;
   makes a written record of a technical assistance request, the Director-General of Security, the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Signals Directorate or the chief officer, as the case requires, must retain the record while the request is in force.

[technical assistance request—written record]

(25) Schedule 1, item 7, page 21 (after line 20), at the end of section 317HAA, add:

Form of advice

(5) Advice under subsection (1), (2), (3) or (4) may be given:
   (a) orally; or
   (b) in writing.

(6) If advice under subsection (1), (2), (3) or (4) is given orally by:
   (a) the Director-General of Security; or
   (b) the Director-General of the Australian Secret Intelligence Service; or
   (c) the Director-General of the Australian Signals Directorate; or
   (d) the chief officer of an interception agency;
   the Director-General of Security, the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Signals Directorate or the chief officer, as the case requires, must:
   (e) make a written record of the advice; and
   (f) do so within 48 hours after the advice was given.

[technical assistance request—form of advice]

(26) Schedule 1, item 7, page 21 (before line 21), before section 317HA, insert:
317HAB Notification obligations

(1) If the Director-General of Security gives a technical assistance request, the Director-General of Security must, within 7 days after the request is given, notify the Inspector-General of Intelligence and Security that the request has been given.

(2) If the Director-General of the Australian Secret Intelligence Service gives a technical assistance request, the Director-General of the Australian Secret Intelligence Service must, within 7 days after the request is given, notify the Inspector-General of Intelligence and Security that the request has been given.

(3) If the Director-General of the Australian Signals Directorate gives a technical assistance request, the Director-General of the Australian Signals Directorate must, within 7 days after the request is given, notify the Inspector-General of Intelligence and Security that the request has been given.

(4) If the chief officer of an interception agency gives a technical assistance request, the chief officer must, within 7 days after the request is given, notify the Commonwealth Ombudsman that the request has been given.

(5) A failure to comply with subsection (1), (2), (3) or (4) does not affect the validity of a technical assistance request.

317JAA Decision-making criteria

(1) The Director-General of Security must not give a technical assistance request to a designated communications provider unless the Director-General of Security is satisfied that:
   (a) the request is reasonable and proportionate; and
   (b) compliance with the request is:
       (i) practicable; and
       (ii) technically feasible.

Note: See also section 317JC.

(2) The Director-General of the Australian Secret Intelligence Service must not give a technical assistance request to a designated communications provider unless the Director-General of the Australian Secret Intelligence Service is satisfied that:
   (a) the request is reasonable and proportionate; and
(b) compliance with the request is:
   (i) practicable; and
   (ii) technically feasible.

Note: See also section 317JC.

(3) The Director-General of the Australian Signals Directorate must not give a technical assistance request to a designated communications provider unless the Director-General of the Australian Signals Directorate is satisfied that:
   (a) the request is reasonable and proportionate; and
   (b) compliance with the request is:
      (i) practicable; and
      (ii) technically feasible.

Note: See also section 317JC.

(4) The chief officer of an interception agency must not give a technical assistance request to a designated communications provider unless the chief officer is satisfied that:
   (a) the request is reasonable and proportionate; and
   (b) compliance with the request is:
      (i) practicable; and
      (ii) technically feasible.

Note: See also section 317JC.

[technical assistance request—decision-making criteria]

(28) Schedule 1, item 7, page 24 (after line 7), at the end of section 317JA, add:

Decision-making criteria

(11) The Director-General of Security must not vary a technical assistance request unless the Director-General of Security is satisfied that:
   (a) the varied request is reasonable and proportionate; and
   (b) compliance with the varied request is:
      (i) practicable; and
      (ii) technically feasible.

Note: See also section 317JC.

(12) The Director-General of the Australian Secret Intelligence Service must not vary a technical assistance request unless the Director-General of the Australian Secret Intelligence Service is satisfied that:
   (a) the varied request is reasonable and proportionate; and
   (b) compliance with the varied request is:
(i) practicable; and
(ii) technically feasible.

Note: See also section 317JC.

(13) The Director-General of the Australian Signals Directorate must not vary a technical assistance request unless the Director-General of the Australian Signals Directorate is satisfied that:
(a) the varied request is reasonable and proportionate; and
(b) compliance with the varied request is:
   (i) practicable; and
   (ii) technically feasible.

Note: See also section 317JC.

(14) The chief officer of an interception agency must not vary a technical assistance request unless the chief officer is satisfied that:
(a) the varied request is reasonable and proportionate; and
(b) compliance with the varied request is:
   (i) practicable; and
   (ii) technically feasible.

Note: See also section 317JC.

Notification obligations

(15) If the Director-General of Security varies a technical assistance request, the Director-General of Security must, within 7 days after varying the request, notify the Inspector-General of Intelligence and Security that the request has been varied.

(16) If the Director-General of the Australian Secret Intelligence Service varies a technical assistance request, the Director-General of the Australian Secret Intelligence Service must, within 7 days after varying the request, notify the Inspector-General of Intelligence and Security that the request has been varied.

(17) If the Director-General of the Australian Signals Directorate varies a technical assistance request, the Director-General of the Australian Signals Directorate must, within 7 days after varying the request, notify the Inspector-General of Intelligence and Security that the request has been varied.

(18) If the chief officer of an interception agency varies a technical assistance request, the chief officer must, within 7 days after varying the request, notify the Commonwealth Ombudsman that the request has been varied.
(19) A failure to comply with subsection (15), (16), (17) or (18) does not affect the validity of a variation of a technical assistance request.  

[technical assistance request—variation]

(29) Schedule 1, item 7, page 24 (after line 11), after subsection 317JB(1), insert:

(1A) If a technical assistance request has been given to a person by the Director-General of Security, and the Director-General of Security is satisfied that:
   (a) the request is not reasonable and proportionate; or
   (b) compliance with the request is not:
       (i) practicable; and
       (ii) technically feasible;
   the Director-General of Security must, by written notice given to the person, revoke the request.

[technical assistance request—revocation]

(30) Schedule 1, item 7, page 24 (after line 15), after subsection 317JB(2), insert:

(2A) If a technical assistance request has been given to a person by the Director-General of the Australian Secret Intelligence Service, and the Director-General of the Australian Secret Intelligence Service is satisfied that:
   (a) the request is not reasonable and proportionate; or
   (b) compliance with the request is not:
       (i) practicable; and
       (ii) technically feasible;
   the Director-General of the Australian Secret Intelligence Service must, by written notice given to the person, revoke the request.

[technical assistance request—revocation]

(31) Schedule 1, item 7, page 24 (after line 19), after subsection 317JB(3), insert:

(3A) If a technical assistance request has been given to a person by the Director-General of the Australian Signals Directorate, and the Director-General of the Australian Signals Directorate is satisfied that:
   (a) the request is not reasonable and proportionate; or
   (b) compliance with the request is not:
       (i) practicable; and
       (ii) technically feasible;
   the Director-General of the Australian Signals Directorate must, by written notice given to the person, revoke the request.

[technical assistance request—revocation]
(32) Schedule 1, item 7, page 24 (after line 22), at the end of section 317JB, add:

(5) If a technical assistance request has been given to a person by the chief officer of an interception agency, and the chief officer is satisfied that:

(a) the request is not reasonable and proportionate; or
(b) compliance with the request is not:
   (i) practicable; and
   (ii) technically feasible;
the chief officer must, by written notice given to the person, revoke the request.

Notification obligations

(6) If the Director-General of Security revokes a technical assistance request, the Director-General of Security must, within 7 days after revoking the request, notify the Inspector-General of Intelligence and Security that the request has been revoked.

(7) If the Director-General of the Australian Secret Intelligence Service revokes a technical assistance request, the Director-General of the Australian Secret Intelligence Service must, within 7 days after revoking the request, notify the Inspector-General of Intelligence and Security that the request has been revoked.

(8) If the Director-General of the Australian Signals Directorate revokes a technical assistance request, the Director-General of the Australian Signals Directorate must, within 7 days after revoking the request, notify the Inspector-General of Intelligence and Security that the request has been revoked.

(9) If the chief officer of an interception agency revokes a technical assistance request, the chief officer must, within 7 days after revoking the request, notify the Commonwealth Ombudsman that the request has been revoked.

(10) A failure to comply with subsection (6), (7), (8) or (9) does not affect the validity of a revocation of a technical assistance request.

[technical assistance request—revocation]

(33) Schedule 1, item 7, page 24 (before line 23), before section 317K, insert:

317JC Whether a technical assistance request is reasonable and proportionate

In considering whether a technical assistance request or a varied technical assistance request is reasonable and proportionate, the Director-General of Security, the Director-General of the Australian

14
Secret Intelligence Service, the Director-General of the Australian Signals Directorate or the chief officer of an interception agency, as the case requires, must have regard to the following matters:

(a) the interests of national security;
(b) the interests of law enforcement;
(c) the legitimate interests of the designated communications provider to whom the request relates;
(d) the objectives of the request;
(e) the availability of other means to achieve the objectives of the request;
(f) whether the request, when compared to other forms of industry assistance known to the Director-General of Security, the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Signals Directorate or the chief officer, as the case requires, is the least intrusive form of industry assistance so far as the following persons are concerned:
   (i) persons whose activities are not of interest to ASIO;
   (ii) persons whose activities are not of interest to the Australian Secret Intelligence Service;
   (iii) persons whose activities are not of interest to the Australian Signals Directorate;
   (iv) persons whose activities are not of interest to interception agencies;
(g) whether the request is necessary;
(h) the legitimate expectations of the Australian community relating to privacy and cybersecurity;
(i) such other matters (if any) as the Director-General of Security, the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Signals Directorate or the chief officer, as the case requires, considers relevant.

[technical assistance request—reasonable and proportionate]

(34) Schedule 1, item 7, page 25 (lines 22 and 23), omit “and laws imposing pecuniary penalties”, substitute “, so far as it relates to serious Australian offences”.

[serious offences]

(35) Schedule 1, item 7, page 25 (line 25), after “country”, insert “, so far as those laws relate to serious foreign offences”.

[serious offences]

(36) Schedule 1, item 7, page 25 (after line 28), after subsection 317L(2), insert:
(2A) The specified acts or things must not be directed towards ensuring that a designated communications provider is capable of giving help to ASIO or an interception agency.

[technical assistance notice—limits]

(37) Schedule 1, item 7, page 25 (line 30), omit “that may be”.

[technical assistance notice—listed acts or things]

(38) Schedule 1, item 7, page 25 (lines 31 and 32), omit “include (but are not limited to)”, substitute “must be”.

[technical assistance notice—listed acts or things]

(39) Schedule 1, item 7, page 26 (after line 4), after section 317L, insert:

317LA Approval of technical assistance notices given by the chief officer of an interception agency of a State or Territory

(1) The chief officer of an interception agency of a State or Territory must not give a technical assistance notice to a designated communications provider unless:

(a) the chief officer has given the AFP Commissioner a written notice setting out a proposal to give the technical assistance notice; and

(b) the AFP Commissioner has approved the giving of the technical assistance notice.

(2) An approval under paragraph (1)(b) may be given:

(a) orally; or

(b) in writing.

(3) If an approval under paragraph (1)(b) is given orally, the AFP Commissioner must:

(a) make a written record of the approval; and

(b) do so within 48 hours after the approval was given.

(4) For the purposes of this section, *AFP Commissioner* means the Commissioner (within the meaning of the *Australian Federal Police Act 1979*).

[technical assistance notice—approval]

(40) Schedule 1, item 7, page 26 (after line 28), at the end of section 317M, add:

(5) If, under subsection (3), the Director-General of Security or the chief officer of an interception agency makes a written record of a technical assistance notice, the Director-General of Security or the chief officer, as the case requires, must retain the record while the notice is in force.
(3) If the Director-General of Security gives a technical assistance notice to a designated communications provider, the Director-General of Security must notify the provider of the provider’s right to make a complaint about the notice to the Inspector-General of Intelligence and Security under the Inspector-General of Intelligence and Security Act 1986.

(4) If:
   (a) the chief officer of an interception agency gives a technical assistance notice to a designated communications provider; and
   (b) the provider has a right to make a complaint about the conduct of the chief officer, or the interception agency, in relation to the notice to:
      (i) the Commonwealth Ombudsman; or
      (ii) an authority that is the State or Territory inspecting agency in relation to the interception agency;
the chief officer must notify the provider of the provider’s right to make such a complaint.

Form of advice or notification

(5) Advice under subsection (1) or (2), or notification under subsection (3) or (4), may be given:
   (a) orally; or
   (b) in writing.

(6) If advice under subsection (1) or (2), or notification under subsection (3) or (4), is given orally by the Director-General of Security or the chief officer of an interception agency, the Director-General of Security or the chief officer, as the case requires, must:
   (a) make a written record of the advice or notification; and
   (b) do so within 48 hours after the advice or notification was given.

(provision of advice to designated communications providers)

(42) Schedule 1, item 7, page 27 (before line 9), before section 317MA, insert:
317MAB Notification obligations

(1) If the Director-General of Security gives a technical assistance notice, the Director-General of Security must, within 7 days after the notice is given, notify the Inspector-General of Intelligence and Security that the notice has been given.

(2) If the chief officer of an interception agency gives a technical assistance notice, the chief officer must, within 7 days after the notice is given, notify the Commonwealth Ombudsman that the notice has been given.

(3) A failure to comply with subsection (1) or (2) does not affect the validity of a technical assistance notice.

(43) Schedule 1, item 7, page 27 (after line 19), after subsection 317MA(1), insert:

(1A) An expiry date specified in a technical assistance notice must not be later than 12 months after the notice was given.

(44) Schedule 1, item 7, page 27 (before line 20), before subsection 317MA(2), insert:

(1B) Paragraph (1)(b) has effect subject to subsections (1C) and (1D).

(1C) If the Director-General of Security has given a technical assistance notice to a designated communications provider, the Director-General of Security may, with the agreement of the provider, extend for a further period (not exceeding 12 months) or further periods (not exceeding 12 months in each case) the period for which the technical assistance notice is in force.

(1D) If the chief officer of an interception agency has given a technical assistance notice to a designated communications provider, the chief officer may, with the agreement of the provider, extend for a further period (not exceeding 12 months) or further periods (not exceeding 12 months in each case) the period for which the technical assistance notice is in force.

(1E) If the Director-General of Security extends the period for which a technical assistance notice is in force, the Director-General of Security must, within 7 days after extending the period, notify the Inspector-General of Intelligence and Security of the extension.
(1F) If the chief officer of an interception agency extends the period for which a technical assistance notice is in force, the chief officer must, within 7 days after extending the period, notify the Commonwealth Ombudsman of the extension.

(1G) A failure to comply with subsection (1E) or (1F) does not affect the validity of an extension of a technical assistance notice.

[technical assistance notice—extension]

(45) Schedule 1, item 7, page 28 (after line 12), after section 317P, insert:

317PA Consultation about a proposal to give a technical assistance notice

(1) Before giving a technical assistance notice to a designated communications provider, the Director-General of Security or the chief officer of an interception agency, as the case requires, must consult the provider.

(2) The rule in subsection (1) does not apply to a technical assistance notice given to a designated communications provider by the Director-General of Security if:

(a) the Director-General of Security is satisfied that the technical assistance notice should be given as a matter of urgency; or

(b) the provider waives compliance with subsection (1).

(3) The rule in subsection (1) does not apply to a technical assistance notice given to a designated communications provider by the chief officer of an interception agency if:

(a) the chief officer is satisfied that the technical assistance notice should be given as a matter of urgency; or

(b) the provider waives compliance with subsection (1).

[technical assistance notice—consultation]

(46) Schedule 1, item 7, page 29 (line 26), omit “that may be”.

[technical assistance notice—listed acts or things]

(47) Schedule 1, item 7, page 29 (line 27), omit “include (but are not limited to)”, substitute “must be”.

[technical assistance notice—listed acts or things]

(48) Schedule 1, item 7, page 30 (after line 11), at the end of section 317Q, add:
Variation must not extend duration of technical assistance notice

(11) A variation of a technical assistance notice must not extend the period for which the notice is in force.

Notification obligations

(12) If the Director-General of Security varies a technical assistance notice, the Director-General of Security must, within 7 days after varying the notice, notify the Inspector-General of Intelligence and Security that the notice has been varied.

(13) If the chief officer of an interception agency varies a technical assistance notice, the chief officer must, within 7 days after varying the notice, notify the Commonwealth Ombudsman that the notice has been varied.

(14) A failure to comply with subsection (12) or (13) does not affect the validity of a variation of a technical assistance notice.

[technical assistance notice—variation]

(49) Schedule 1, item 7, page 31 (after line 4), at the end of section 317R, add:

Notification obligations

(5) If the Director-General of Security revokes a technical assistance notice, the Director-General of Security must, within 7 days after revoking the notice, notify the Inspector-General of Intelligence and Security that the notice has been revoked.

(6) If the chief officer of an interception agency revokes a technical assistance notice, the chief officer must, within 7 days after revoking the notice, notify the Commonwealth Ombudsman that the notice has been revoked.

(7) A failure to comply with subsection (5) or (6) does not affect the validity of a revocation of a technical assistance notice.

[technical assistance notice—revocation]

(50) Schedule 1, item 7, page 31 (after line 18), after paragraph 317RA(e), insert:

(ea) whether the requirements, when compared to other forms of industry assistance known to the Director-General of Security or the chief officer, as the case requires, are the least intrusive form of industry assistance so far as the following persons are concerned:

(i) persons whose activities are not of interest to ASIO;
(ii) persons whose activities are not of interest to interception agencies;

(eb) whether the requirements are necessary;

[technical assistance notice—whether requirements are reasonable and proportionate]

(51) Schedule 1, item 7, page 33 (lines 3 and 4), omit “and laws imposing pecuniary penalties”, substitute “, so far as it relates to serious Australian offences”.

[serious offences]

(52) Schedule 1, item 7, page 33 (line 6), after “country”, insert “, so far as those laws relate to serious foreign offences”.

[serious offences]

(53) Schedule 1, item 7, page 33 (line 23), before “Minister”, insert “Home Affairs”.

[Home Affairs Minister]

(54) Schedule 1, item 7, page 33 (line 26), before “Minister”, insert “Home Affairs”.

[Home Affairs Minister]

(55) Schedule 1, item 7, page 33 (line 33), before “Minister”, insert “Home Affairs”.

[Home Affairs Minister]

(56) Schedule 1, item 7, page 34 (line 2), omit “that may be”.

[technical capability notice—listed acts or things]

(57) Schedule 1, item 7, page 34 (line 4), omit “include (but are not limited to)”, substitute “must be”.

[technical capability notice—listed acts or things]

(58) Schedule 1, item 7, page 34 (line 10) to page 35 (line 13), omit subsections 317T(8) to (11).

[technical capability notice—limits]

(59) Schedule 1, item 7, page 35 (after line 21), after section 317T, insert:

317TAAA Approval of technical capability notice

(1) The Attorney-General must not give a technical capability notice to a designated communications provider unless:
(a) the Attorney-General has given the Minister a written notice setting out a proposal to give the technical capability notice; and
(b) the Minister has approved the giving of the technical capability notice.

(2) An approval under paragraph (1)(b) may be given:
   (a) orally; or
   (b) in writing.

(3) If an approval under paragraph (1)(b) is given orally, the Minister must:
   (a) make a written record of the approval; and
   (b) do so within 48 hours after the approval was given.

(4) The Attorney-General may make a representation to the Minister about the proposal to give the technical capability notice.

(5) A representation may deal with:
   (a) any of the matters set out in section 317ZAA; and
   (b) such other matters (if any) as the Attorney-General considers relevant.

(6) In considering whether to approve the giving of the technical capability notice, the Minister must have regard to the following matters:
   (a) the objectives of the notice;
   (b) the legitimate interests of the designated communications provider to whom the notice relates;
   (c) the impact of the notice on the efficiency and international competitiveness of the Australian telecommunications industry;
   (d) the representation (if any) that was made under subsection (4);
   (e) such other matters (if any) as the Minister considers relevant.

[technical capability notice—approval]

(60) Schedule 1, item 7, page 35 (line 24), before “If”, insert “(1)”.

[provision of advice to designated communications providers]

(61) Schedule 1, item 7, page 35 (after line 28), at the end of section 317TAA, add:

Form of advice

(2) Advice under subsection (1) may be given:
   (a) orally; or
   (b) in writing.
(3) If advice under subsection (1) is given orally, the Attorney-General must:
   (a) make a written record of the advice; and
   (b) do so within 48 hours after the advice was given.

(provision of advice to designated communications providers)

(62) Schedule 1, item 7, page 35 (before line 29), before section 317TA, insert:

317TAB Notification obligations

(1) If:
   (a) the Attorney-General gives a technical capability notice; and
   (b) the acts or things specified in the notice:
      (i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or
      (ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b);
   the Attorney-General must, within 7 days after the notice is given, notify the Inspector-General of Intelligence and Security that the notice has been given.

(2) If:
   (a) the Attorney-General gives a technical capability notice; and
   (b) the acts or things specified in the notice:
      (i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to an interception agency in relation to a matter covered by paragraph 317T(2)(a); or
      (ii) are by way of giving help to an interception agency in relation to a matter covered by paragraph 317T(2)(b);
   the Attorney-General must, within 7 days after the notice is given, notify the Commonwealth Ombudsman that the notice has been given.

(3) A failure to comply with subsection (1) or (2) does not affect the validity of a technical capability notice.

(63) Schedule 1, item 7, page 36 (after line 7), after subsection 317TA(1), insert:

(1A) An expiry date specified in a technical capability notice must not be later than 12 months after the notice was given.

(technical capability notice—expiry date)
Paragraph (1)(b) has effect subject to subsection (1C).

(1C) If the Attorney-General has given a technical capability notice to a designated communications provider, the Attorney-General may, with the agreement of the provider, extend for a further period (not exceeding 12 months) or further periods (not exceeding 12 months in each case) the period for which the technical capability notice is in force.

(1D) If:

(a) the Attorney-General extends the period for which a technical capability notice is in force; and

(b) the acts or things specified in the notice:

(i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or

(ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b);

the Attorney-General must, within 7 days after extending the period, notify the Inspector-General of Intelligence and Security of the extension.

(1E) If:

(a) the Attorney-General extends the period for which a technical capability notice is in force; and

(b) the acts or things specified in the notice:

(i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to an interception agency in relation to a matter covered by paragraph 317T(2)(a); or

(ii) are by way of giving help to an interception agency in relation to a matter covered by paragraph 317T(2)(b);

the Attorney-General must, within 7 days after extending the period, notify the Commonwealth Ombudsman of the extension.

(1F) A failure to comply with subsection (1D) or (1E) does not affect the validity of an extension of a technical capability notice.

[technical capability notice—extension]

(65) Schedule 1, item 7, page 37 (line 13), omit “; and”, substitute “.”.
(66) Schedule 1, item 7, page 37 (lines 14 to 16), omit paragraph 317W(1)(c).

(67) Schedule 1, item 7, page 38 (lines 3 to 32), omit subsections 317W(7) to (11), substitute:

(7) Subsection (1) does not apply to a technical capability notice proposed to be given to a designated communications provider if:
   (a) the requirements imposed by the proposed technical capability notice are the same, or substantially the same, as the requirements imposed by another technical capability notice that has previously been given to the provider; and
   (b) the proposed technical capability notice is to come into force immediately after the expiry of the other technical capability notice.

Special consultation requirements for replacement technical capability notices

(8) Before giving a designated communications provider a technical capability notice that satisfies the following conditions:
   (a) the requirements imposed by the technical capability notice are the same, or substantially the same, as the requirements imposed by another technical capability notice that has previously been given to the provider;
   (b) the first-mentioned technical capability notice is to come into force immediately after the expiry of the other technical capability notice;
   the Attorney-General must consult the provider.

(9) The rule in subsection (8) does not apply to a technical capability notice given to a designated communications provider if the provider waives compliance with subsection (8).

(68) Schedule 1, item 7, page 38 (after line 32), after section 317W, insert:

317WA Assessment and report

Designated communications provider may request carrying out of assessment

(1) If a consultation notice is given to a designated communications provider under subsection 317W(1) in relation to a proposed technical
capability notice, the provider may, within the time limit specified in the consultation notice, give the Attorney-General a written notice requesting the carrying out of an assessment of whether the proposed technical capability notice should be given.

**Attorney-General must appoint assessors**

(2) If a designated communications provider gives the Attorney-General a notice under subsection (1) in relation to a proposed technical capability notice, the Attorney-General must appoint 2 persons to carry out an assessment of whether the proposed technical capability notice should be given.

(3) For the purposes of this section, the persons appointed under subsection (2) are to be known as the *assessors*.

(4) One of the assessors must be a person who:
   (a) has knowledge that would enable the person to assess whether proposed technical capability notices would contravene section 317ZG; and
   (b) is cleared for security purposes to:
       (i) the highest level required by staff members of ASIO; or
       (ii) such lower level as the Attorney-General approves.

(5) One of the assessors must be a person who:
   (a) has served as a judge in one or more prescribed courts for a period of 5 years; and
   (b) no longer holds a commission as a judge of a prescribed court.

**Assessment and report by assessors**

(6) As soon as practicable after being appointed under subsection (2), the assessors must:
   (a) carry out an assessment of whether the proposed technical capability notice should be given; and
   (b) prepare a report of the assessment; and
   (c) give a copy of the report to:
       (i) the Attorney-General; and
       (ii) the designated communications provider concerned; and
   (d) if the acts or things specified in the proposed technical capability notice:
       (i) are directed towards ensuring that the designated communications provider is capable of giving listed help (within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or
(ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b);
give a copy of the report to the Inspector-General of Intelligence and Security; and
(e) if the acts or things specified in the proposed technical capability notice:
   (i) are directed towards ensuring that the designated communications provider is capable of giving listed help (within the meaning of section 317T) to an interception agency in relation to a matter covered by paragraph 317T(2)(a); or
   (ii) are by way of giving help to an interception agency in relation to a matter covered by paragraph 317T(2)(b);
give a copy of the report to the Commonwealth Ombudsman.

(7) In carrying out an assessment under paragraph (6)(a) in relation to a technical capability notice proposed to be given to a designated communications provider, the assessors must:
   (a) consider:
      (i) whether the proposed technical capability notice would contravene section 317ZG; and
      (ii) whether the requirements imposed by the proposed technical capability notice are reasonable and proportionate; and
      (iii) whether compliance with the proposed technical capability notice is practicable; and
      (iv) whether compliance with the proposed technical capability notice is technically feasible; and
      (v) whether the proposed technical capability notice is the least intrusive measure that would be effective in achieving the legitimate objective of the proposed technical capability notice; and
   (b) give the greatest weight to the matter mentioned in subparagraph (a)(i).

(8) In carrying out an assessment under paragraph (6)(a) in relation to a technical capability notice proposed to be given to a designated communications provider, the assessors must consult:
   (a) the provider; and
   (b) if the acts or things specified in the proposed technical capability notice:
      (i) are directed towards ensuring that a designated communications provider is capable of giving listed help
(within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or
(ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b);
the Director-General of Security; and
(c) if the acts or things specified in the proposed technical capability notice:
   (i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to an interception agency in relation to a matter covered by paragraph 317T(2)(a); or
   (ii) are by way of giving help to an interception agency in relation to a matter covered by paragraph 317T(2)(b);
the chief officer of the interception agency.

(9) If:
   (a) the assessors have begun to carry out an assessment under paragraph (6)(a) in relation to a technical capability notice proposed to be given to a designated communications provider; and
   (b) the provider informs the Attorney-General that the provider no longer wants the assessment to be carried out;
then:
   (c) the Attorney-General must direct the assessors to cease carrying out the assessment; and
   (d) the assessors must comply with the direction.

(10) If:
   (a) the assessors have begun to carry out an assessment under paragraph (6)(a); and
   (b) the Attorney-General withdraws the proposed technical capability notice to which the assessment relates;
then:
   (c) the Attorney-General must direct the assessors to cease carrying out the assessment; and
   (d) the assessors must comply with the direction.

Attorney-General must have regard to the report of the assessment

(11) If:
   (a) a notice is given under subsection (1) in relation to a technical capability notice proposed to be given to a designated communications provider; and
(b) a copy of the report relating to the proposed technical capability notice is given to the Attorney-General under subsection (6); the Attorney-General, in considering whether to proceed to give the technical capability notice, must have regard to the copy of the report.

**Technical capability notice information**

(12) For the purposes of this Part:
   (a) information about the carrying out of an assessment under subsection (6); or
   (b) information contained in a report prepared under subsection (6); is taken to be information about consultation relating to the giving of a technical capability notice.

**Prescribed court**

(13) For the purposes of this section, **prescribed court** means:
   (a) the High Court; or
   (b) the Federal Court of Australia; or
   (c) the Supreme Court of a State or Territory; or
   (d) the District Court (or equivalent) of a State or Territory.

**[technical capability notice—assessment and report]**

(69) Schedule 1, item 7, page 39 (line 11), omit “that may be”.

**[technical capability notice—listed acts or things]**

(70) Schedule 1, item 7, page 39 (lines 12 and 13), omit “include (but are not limited to)”, substitute “must be”.

**[technical capability notice—listed acts or things]**

(71) Schedule 1, item 7, page 39 (after line 28), at the end of section 317X, add:

*Variation must not extend duration of technical capability notice*

(5) A variation of a technical capability notice must not extend the period for which the notice is in force.

**Notification obligations**

(6) If:
   (a) the Attorney-General varies a technical capability notice; and
   (b) the acts or things specified in the varied notice:
      (i) are directed towards ensuring that a designated communications provider is capable of giving listed help
(within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or

(ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b);

the Attorney-General must, within 7 days after varying the notice, notify the Inspector-General of Intelligence and Security that the notice has been varied.

(7) If:

(a) the Attorney-General varies a technical capability notice; and

(b) the acts or things specified in the varied notice:

(i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to an interception agency in relation to a matter covered by paragraph 317T(2)(a); or

(ii) are by way of giving help to an interception agency in relation to a matter covered by paragraph 317T(2)(b);

the Attorney-General must, within 7 days after varying the notice, notify the Commonwealth Ombudsman that the notice has been varied.

(8) A failure to comply with subsection (6) or (7) does not affect the validity of a variation of a technical capability notice.

[technical capability notice—variation]

(72) Schedule 1, item 7, page 40 (before line 1), before section 317Y, insert:

317XA Approval of variation of technical capability notice

(1) If a technical capability notice has been given to a designated communications provider, the Attorney-General must not vary the notice unless:

(a) both:

(i) the Attorney-General has given the Minister a written notice setting out a proposal to vary the technical capability notice; and

(ii) the Minister has approved the variation of the technical capability notice; or

(b) the provider has waived compliance with subsection 317Y(2) in relation to the variation of the technical capability notice.

(2) An approval under subparagraph (1)(a)(ii) may be given:

(a) orally; or

(b) in writing.
(3) If an approval under subparagraph (1)(a)(ii) is given orally, the
Minister must:
   (a) make a written record of the approval; and
   (b) do so within 48 hours after the approval was given.

(4) The Attorney-General may make a representation to the Minister about
the proposal to vary the technical capability notice.

(5) A representation may deal with:
   (a) any of the matters set out in section 317ZAA; and
   (b) such other matters (if any) as the Attorney-General considers
       relevant.

(6) In considering whether to approve the variation of the technical
capability notice, the Minister must have regard to the following
matters:
   (a) the objectives of the notice as proposed to be varied;
   (b) the legitimate interests of the designated communications
       provider to whom the notice relates;
   (c) the impact of the notice as proposed to be varied on the
       efficiency and international competitiveness of the Australian
       telecommunications industry;
   (d) the representation (if any) that was made under subsection (4);
   (e) such other matters (if any) as the Minister considers relevant.

   [variation of technical capability notice—approval]

(73) Schedule 1, item 7, page 40 (after line 33), after section 317Y, insert:

317YA Assessment and report

Designated communications provider may request carrying out of
assessment

(1) If:
   (a) a consultation notice is given to a designated communications
       provider under subsection 317Y(1) in relation to a proposed
       variation of a technical capability notice; and
   (b) the variation is not of a minor nature;
the provider may, within the time limit specified in the consultation
notice, give the Attorney-General a written notice requesting the
carrying out of an assessment of whether the technical capability notice
as proposed to be varied would contravene section 317ZG.
Attorney-General must appoint assessors

(2) If a designated communications provider gives the Attorney-General a notice under subsection (1) in relation to a technical capability notice as proposed to be varied, the Attorney-General must appoint 2 persons to carry out an assessment of whether the technical capability notice as proposed to be varied would contravene section 317ZG.

(3) For the purposes of this section, the persons appointed under subsection (2) are to be known as the assessors.

(4) One of the assessors must be a person who:
   (a) has knowledge that would enable the person to assess whether proposed technical capability notices would contravene section 317ZG; and
   (b) is cleared for security purposes to:
       (i) the highest level required by staff members of ASIO; or
       (ii) such lower level as the Attorney-General approves.

(5) One of the assessors must be a person who:
   (a) has served as a judge in one or more prescribed courts for a period of 5 years; and
   (b) no longer holds a commission as a judge of a prescribed court.

Assessment and report by assessors

(6) As soon as practicable after being appointed under subsection (2), the assessors must:
   (a) carry out an assessment of whether the technical capability notice as proposed to be varied would contravene section 317ZG; and
   (b) prepare a report of the assessment; and
   (c) give a copy of the report to:
       (i) the Attorney-General; and
       (ii) the designated communications provider concerned; and
   (d) if the acts or things specified in the technical capability notice as proposed to be varied:
       (i) are directed towards ensuring that the designated communications provider is capable of giving listed help (within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or
       (ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b);
       give a copy of the report to the Inspector-General of Intelligence and Security; and
(e) if the acts or things specified in the technical capability notice as
proposed to be varied:
   (i) are directed towards ensuring that the designated
       communications provider is capable of giving listed help
       (within the meaning of section 317T) to an interception
       agency in relation to a matter covered by
       paragraph 317T(2)(a); or
   (ii) are by way of giving help to an interception agency in
       relation to a matter covered by paragraph 317T(2)(b);
       give a copy of the report to the Commonwealth Ombudsman.

(7) In carrying out an assessment under paragraph (6)(a) in relation to a
technical capability notice as proposed to be varied, the assessors must consult:
   (a) the designated communications provider concerned; and
   (b) if the acts or things specified in the technical capability notice as
       proposed to be varied:
       (i) are directed towards ensuring that the designated
           communications provider is capable of giving listed help
           (within the meaning of section 317T) to ASIO in relation to
           a matter covered by paragraph 317T(2)(a); or
       (ii) are by way of giving help to ASIO in relation to a matter
           covered by paragraph 317T(2)(b);
           the Director-General of Security; and
   (c) if the acts or things specified in the technical capability notice as
       proposed to be varied:
       (i) are directed towards ensuring that the designated
           communications provider is capable of giving listed help
           (within the meaning of section 317T) to an interception
           agency in relation to a matter covered by
           paragraph 317T(2)(a); or
       (ii) are by way of giving help to an interception agency in
           relation to a matter covered by paragraph 317T(2)(b);
           the chief officer of the interception agency.

(8) If:
   (a) the assessors have begun to carry out an assessment under
       paragraph (6)(a) in relation to the technical capability notice as
       proposed to be varied; and
   (b) the designated communications provider concerned informs the
       Attorney-General that the provider no longer wants the
       assessment to be carried out;

then:
(c) the Attorney-General must direct the assessors to cease carrying out the assessment; and
(d) the assessors must comply with the direction.

(9) If:
(a) the assessors have begun to carry out an assessment under paragraph (6)(a); and
(b) the Attorney-General withdraws the proposed variation of the technical capability notice concerned;
then:
(c) the Attorney-General must direct the assessors to cease carrying out the assessment; and
(d) the assessors must comply with the direction.

Attorney-General must have regard to the report of the assessment

(10) If:
(a) a notice is given under subsection (1) in relation to a proposed variation of a technical capability notice; and
(b) a copy of the report relating to the technical capability notice as proposed to be varied is given to the Attorney-General under subsection (6);
the Attorney-General, in considering whether to proceed to vary the technical capability notice, must have regard to the copy of the report.

Technical capability notice information

(11) For the purposes of this Part:
(a) information about the carrying out of an assessment under subsection (6); or
(b) information contained in a report prepared under subsection (6);
is taken to be information about consultation relating to the variation of a technical capability notice.

Prescribed court

(12) For the purposes of this section, prescribed court means:
(a) the High Court; or
(b) the Federal Court of Australia; or
(c) the Supreme Court of a State or Territory; or
(d) the District Court (or equivalent) of a State or Territory.

[Variation of technical capability notice—assessment and report]

(74) Schedule 1, item 7, page 41 (after line 13), at the end of section 317Z, add:
Notification obligations

(3) If:
   (a) the Attorney-General revokes a technical capability notice; and
   (b) the acts or things specified in the revoked notice:
       (i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or
       (ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b);
the Attorney-General must, within 7 days after revoking the notice, notify the Inspector-General of Intelligence and Security that the notice has been revoked.

(4) If:
   (a) the Attorney-General revokes a technical capability notice; and
   (b) the acts or things specified in the revoked notice:
       (i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to an interception agency in relation to a matter covered by paragraph 317T(2)(a); or
       (ii) are by way of giving help to an interception agency in relation to a matter covered by paragraph 317T(2)(b);
the Attorney-General must, within 7 days after revoking the notice, notify the Commonwealth Ombudsman that the notice has been revoked.

(5) A failure to comply with subsection (3) or (4) does not affect the validity of a revocation of a technical capability notice.

[technical capability notice—revocation]

(75) Schedule 1, item 7, page 41 (after line 26), after paragraph 317ZAA(e), insert:

   (ea) whether the requirements, when compared to other forms of industry assistance known to the Attorney-General, are the least intrusive form of industry assistance so far as the following persons are concerned:
       (i) persons whose activities are not of interest to ASIO;
       (ii) persons whose activities are not of interest to interception agencies;
   (eb) whether the requirements are necessary;
(76) Schedule 1, item 7, page 46 (line 9), omit subparagraph 317ZF(1)(b)(x), substitute:

(x) a person appointed under subsection 317WA(2); or
(xa) a person appointed under subsection 317YA(2); or

[unauthorised disclosure of information]

(77) Schedule 1, item 7, page 47 (after line 13), after subparagraph 317ZF(1)(d)(ix), insert:

(ixa) if the person is or was a person appointed under
subsection 317WA(2)—in the person’s capacity as such an
appointee; or
(ixb) if the person is or was a person appointed under
subsection 317YA(2)—in the person’s capacity as such an
appointee; or

[unauthorised disclosure of information]

(78) Schedule 1, item 7, page 48 (line 3), after ““(5),””, insert ““(5A), (5B), (5C)”.

[unauthorised disclosure of information]

(79) Schedule 1, item 7, page 48 (line 3), omit “or (13)”, substitute “, (12A),
(12B), (12C), (12D), (13), (14), (15) or (16)”.

[unauthorised disclosure of information]

(80) Schedule 1, item 7, page 48 (line 4), omit “A defendant”, substitute “Except
as provided by subsection (2A) or (2B), a defendant”.

[unauthorised disclosure of information]

(81) Schedule 1, item 7, page 48 (after line 5), after subsection 317ZF(2), insert:

(2A) Despite subsection 13.3(3) of the Criminal Code, in a prosecution for
an offence against subsection (1) of this section, an IGIS official does
not bear an evidential burden in relation to the matters in subsection (2)
of this section, to the extent to which that subsection relates to
subsection (5) of this section.

(2B) Despite subsection 13.3(3) of the Criminal Code, in a prosecution for
an offence against subsection (1) of this section, an Ombudsman
official does not bear an evidential burden in relation to the matters in
subsection (2) of this section, to the extent to which that subsection
relates to subsection (5A), (5B) or (5C) of this section.

[unauthorised disclosure of information]
(82) Schedule 1, item 7, page 48 (line 26), at the end of subsection 317ZF(3), add: 

; or (g) to an Ombudsman official for the purpose of exercising powers, or performing functions or duties, as an Ombudsman official. 

[unauthorised disclosure of information]

(83) Schedule 1, item 7, page 49 (after line 4), after subsection 317ZF(5), insert:

Authorised disclosures—Ombudsman official

(5A) An Ombudsman official may disclose:

(a) technical assistance notice information; or

(b) technical capability notice information; or

(c) technical assistance request information;
in connection with the Ombudsman official exercising powers, or performing functions or duties, as an Ombudsman official.

(5B) If a technical assistance notice is given by the chief officer of an interception agency of a State or Territory, an Ombudsman official may disclose technical assistance notice information that relates to the notice to an officer or employee of an authority that is the State or Territory inspecting authority in relation to the interception agency, so long as the disclosure is in connection with the officer or employee exercising powers, or performing functions or duties, as an officer or employee of the State or Territory inspecting authority.

(5C) If a technical assistance request is given by the chief officer of an interception agency of a State or Territory, an Ombudsman official may disclose technical assistance request information that relates to the request to an officer or employee of an authority that is the State or Territory inspecting authority in relation to the interception agency, so long as the disclosure is in connection with the officer or employee exercising powers, or performing functions or duties, as an officer or employee of the State or Territory inspecting authority.

[unauthorised disclosure of information]

(84) Schedule 1, item 7, page 50 (after line 29), after subsection 317ZF(12), insert:

Authorised disclosures—Communications Access Co-ordinator

(12A) If:

(a) the Attorney-General has given a technical capability notice; and

(b) the acts or things specified in the notice:

(i) are directed towards ensuring that a designated communications provider is capable of giving listed help
(within the meaning of section 317T) to an interception agency of a State or Territory in relation to a matter covered by paragraph 317T(2)(a); or

(ii) are by way of giving help to an interception agency of a State or Territory in relation to a matter covered by paragraph 317T(2)(b);

the Communications Access Co-ordinator may disclose technical capability notice information that relates to the notice to an officer or employee of an authority that is the State or Territory inspecting authority in relation to the interception agency, so long as the disclosure is in connection with the officer or employee exercising powers, or performing functions or duties, as an officer or employee of the State or Territory inspecting authority.

Authorised disclosures—State or Territory inspecting authority

(12B) If a technical assistance notice has been given to a designated communications provider by the chief officer of an interception agency of a State or Territory:

(a) the designated communications provider; or

(b) an employee of the designated communications provider; or

(c) a contracted service provider of the designated communications provider; or

(d) an employee of a contracted service provider of the designated communications provider;

may disclose technical assistance notice information that relates to the notice to an officer or employee of an authority that is the State or Territory inspecting authority in relation to the interception agency, so long as the disclosure is in connection with the officer or employee exercising powers, or performing functions or duties, as an officer or employee of the State or Territory inspecting authority.

(12C) If a technical assistance request has been given to a designated communications provider by the chief officer of an interception agency of a State or Territory:

(a) the designated communications provider; or

(b) an employee of the designated communications provider; or

(c) a contracted service provider of the designated communications provider; or

(d) an employee of a contracted service provider of the designated communications provider;

may disclose technical assistance request information that relates to the request to an officer or employee of an authority that is the State or Territory inspecting authority in relation to the interception agency, so
long as the disclosure is in connection with the officer or employee exercising powers, or performing functions or duties, as an officer or employee of the State or Territory inspecting authority.

(12D) If:

(a) technical assistance notice information is disclosed under subsection (12B); or

(b) technical assistance request information is disclosed under subsection (12C);

to an officer or employee of an authority that is the State or Territory inspecting authority in relation to an interception agency, the officer or employee may disclose the information in connection with the officer or employee exercising powers, or performing functions or duties, as an officer or employee of the State or Territory inspecting authority.

[unauthorised disclosure of information]

(85) Schedule 1, item 7, page 51 (after line 16), at the end of section 317ZF, add:

Other authorised disclosures

(14) If a technical assistance notice has been given to a designated communications provider by the Director-General of Security, the Director-General of Security may, if requested to do so by the designated communications provider, authorise:

(a) the designated communications provider; or

(b) a specified employee of the designated communications provider; or

(c) a specified contracted service provider of the designated communications provider; or

(d) a specified employee of a contracted service provider of the designated communications provider;

to disclose, in accordance with the conditions specified in the authorisation, specified technical assistance notice information that relates to the notice.

(15) If a technical assistance notice has been given to a designated communications provider by the chief officer of an interception agency, the chief officer may, if requested to do so by the designated communications provider, authorise:

(a) the designated communications provider; or

(b) a specified employee of the designated communications provider; or

(c) a specified contracted service provider of the designated communications provider; or

39
(d) a specified employee of a contracted service provider of the designated communications provider;

to disclose, in accordance with the conditions specified in the authorisation, specified technical assistance notice information that relates to the notice.

(16) If a technical capability notice has been given to a designated communications provider, the Attorney-General may, if requested to do so by the designated communications provider, authorise:

(a) the designated communications provider; or

(b) a specified employee of the designated communications provider; or

(c) a specified contracted service provider of the designated communications provider; or

(d) a specified employee of a contracted service provider of the designated communications provider;

to disclose, in accordance with the conditions specified in the authorisation, specified technical capability notice information that relates to the notice.

(17) An authorisation under subsection (14), (15) or (16) must be in writing.

[unauthorised disclosure of information]

(86) Schedule 1, item 7, page 52 (line 2), before “required”, insert “requested or”.

[systemic vulnerability and systemic weakness]

(87) Schedule 1, item 7, page 52 (line 5), before “technical assistance notice”, insert “technical assistance request,”.

[systemic vulnerability and systemic weakness]

(88) Schedule 1, item 7, page 52 (line 7), before “requiring”, insert “requesting or”.

[systemic vulnerability and systemic weakness]

(89) Schedule 1, item 7, page 52 (after line 22), after subsection 317ZG(4), insert:

(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.
(4B) In a case where a vulnerability is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic vulnerability into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.

(4C) For the purposes of subsections (4A) and (4B), an act or thing will, or is likely to, jeopardise the security of information if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party.

[systemic weakness and systemic vulnerability]

(90) Schedule 1, item 7, page 52 (line 23), before “technical assistance notice”, insert “technical assistance request,”.

[systemic vulnerability and systemic weakness]

(91) Schedule 1, item 7, page 52 (after line 25), after section 317ZG, insert:

317ZGA Limits on technical capability notices

(1) If:
   (a) a designated communications provider supplies a particular kind of telecommunications service; and
   (b) the service involves, or will involve, the use of a telecommunications system;

a technical capability notice has no effect to the extent (if any) to which it requires the provider to ensure that the kind of service, or the system:
   (c) has the capability to enable a communication passing over the system to be intercepted in accordance with an interception warrant; or
   (d) has the capability to transmit lawfully intercepted information to the delivery points applicable in respect of that kind of service; or
   (e) has a delivery capability.

Note 1: Part 5-3 of the Telecommunications (Interception and Access) Act 1979 deals with interception capability.

Note 2: Part 5-5 of the Telecommunications (Interception and Access) Act 1979 deals with delivery capability.

(2) For the purposes of subsection (1), ensuring that a kind of service or a system has a particular capability includes ensuring that the capability is developed, installed and maintained.
A technical capability notice has no effect to the extent (if any) to which it requires a designated communications provider to keep, or cause to be kept:

(a) information of a kind specified in or under section 187AA of the *Telecommunications (Interception and Access) Act 1979*; or

(b) documents containing information of that kind;

relating to any communication carried by means of a service to which Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* applies.

Note: Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* deals with data retention.

A technical capability notice has no effect to the extent (if any) to which it requires a designated communications provider to keep, or cause to be kept, information that:

(a) states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the provider; and

(b) was obtained by the provider only as a result of providing the service.

Note: This subsection ensures that a technical capability notice cannot require a designated communications provider to keep information about subscribers’ web browsing history.

An expression used in this section and in Chapter 5 of the *Telecommunications (Interception and Access) Act 1979* has the same meaning in this section as it has in that Chapter.

**[technical capability notice—limits]**

(92) Schedule 1, item 7, page 52 (line 26), before “technical assistance notices”, insert “technical assistance requests,”.

**[general limits on technical assistance requests, technical assistance notices and technical capability notices]**

(93) Schedule 1, item 7, page 52 (line 28), after “A”, insert “technical assistance request that relates to an agency, or a”.

**[general limits on technical assistance requests, technical assistance notices and technical capability notices]**

(94) Schedule 1, item 7, page 52 (line 28), after “technical assistance notice”, insert “that relates to an agency,”.

**[general limits on technical assistance requests, technical assistance notices and technical capability notices]**

(95) Schedule 1, item 7, page 52 (line 28), after “or”, insert “a”.

42
Schedule 1, item 7, page 52 (line 28), after “technical capability notice”, insert “that relates to an agency,”.

Schedule 1, item 7, page 52 (line 29), before “require”, insert “request or”.

Schedule 1, item 7, page 52 (line 30), after “for which”, insert “the agency, or an officer of the agency, would be required to have or obtain”.

Schedule 1, item 7, page 52 (line 31), omit “is required”.

Schedule 1, item 7, page 53 (line 3), omit paragraph 317ZH(1)(e).

Schedule 1, item 7, page 53 (line 5), omit “, (d) or (e)”, substitute “or (d)”.

Schedule 1, item 7, page 53 (line 13), before “technical assistance notice”, insert “technical assistance request,”.

Schedule 1, item 7, page 53 (line 14), before “require”, insert “request or”.

Schedule 1, item 7, page 53 (line 22), before “technical”, insert “technical assistance request,”.

Schedule 1, item 7, page 53 (line 23), before “requiring”, insert “requesting or”.

43
(106) Schedule 1, item 7, page 53 (before line 29), before paragraph 317ZH(4)(c), insert:

(c) in the case of a technical assistance request—a matter covered by subparagraph 317G(2)(b)(v) or (vi); or

(107) Schedule 1, item 7, page 54 (after line 16), at the end of section 317ZH, add:

Interpretation

(6) For the purposes of this section, a technical assistance request relates to an agency if:

(a) if the agency is ASIO—the request was given by the Director-General of Security; or

(b) if the agency is the Australian Secret Intelligence Service—the request was given by the Director-General of the Australian Secret Intelligence Service; or

(c) if the agency is the Australian Signals Directorate—the request was given by the Director-General of the Australian Signals Directorate; or

(d) if the agency is an interception agency—the request was given by the chief officer of the interception agency.

(7) For the purposes of this section, a technical assistance notice relates to an agency if:

(a) if the agency is ASIO—the notice was given by the Director-General of Security; or

(b) if the agency is an interception agency—the notice was given by the chief officer of the interception agency.

(8) For the purposes of this section, a technical capability notice relates to an agency if:

(a) if the agency is ASIO—the acts or things specified in the notice:

(i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or

(ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b); or

(b) if the agency is an interception agency—the acts or things specified in the notice:
(i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to the interception agency in relation to a matter covered by paragraph 317T(2)(a); or
(ii) are by way of giving help to the interception agency in relation to a matter covered by paragraph 317T(2)(b).

(9) For the purposes of this section, agency means:
   (a) ASIO; or
   (b) the Australian Secret Intelligence Service; or
   (c) the Australian Signals Directorate; or
   (d) an interception agency.

(10) For the purposes of this section, officer of an agency means:
   (a) if the agency is ASIO:
      (i) the Director-General of Security; or
      (ii) an ASIO employee; or
   (b) if the agency is the Australian Secret Intelligence Service:
      (i) the Director-General of the Australian Secret Intelligence Service; or
      (ii) a staff member of the Australian Secret Intelligence Service; or
   (c) if the agency is the Australian Signals Directorate:
      (i) the Director-General of the Australian Signals Directorate; or
      (ii) a staff member of the Australian Signals Directorate; or
   (d) if the agency is an interception agency:
      (i) the chief officer of the interception agency; or
      (ii) an officer of the interception agency.

[general limits on technical assistance requests, technical assistance notices and technical capability notices]

(108) Schedule 1, item 7, page 55 (line 17), after “Director-General of Security”,
insert “declares in writing that the Director-General of Security”.

[terms and conditions on which help is to be given]

(109) Schedule 1, item 7, page 55 (line 22), after “chief officer”, insert “declares in writing that the chief officer”.

[terms and conditions on which help is to be given]

(110) Schedule 1, item 7, page 55 (line 25), after “Attorney-General”, insert “declares in writing that the Attorney-General”.

45
(111) Schedule 1, item 7, page 55 (line 32), before “the interests”, insert “in the case of a requirement under a technical assistance notice given by the chief officer of an interception agency or a requirement under a technical capability notice that relates to an interception agency—”.

(112) Schedule 1, item 7, page 55 (line 33), before “the interests”, insert “in the case of a requirement under a technical assistance notice given by the Director-General of Security or a requirement under a technical capability notice that relates to ASIO—”.

(113) Schedule 1, item 7, page 56 (lines 14 and 15), omit “unless the provider and the applicable costs negotiator otherwise agree.”, substitute:

unless:

(c) the provider and the applicable costs negotiator otherwise agree; or

(d) in the case of a requirement under a technical assistance notice given by the Director-General of Security—the Director-General of Security declares in writing that the Director-General of Security is satisfied that it would be contrary to the public interest for this subsection to apply to the requirement; or

(e) in the case of a requirement under a technical assistance notice given by the chief officer of an interception agency—the chief officer declares in writing that the chief officer is satisfied that it would be contrary to the public interest for this subsection to apply to the requirement; or

(f) in the case of a requirement under a technical capability notice—the Attorney-General declares in writing that the Attorney-General is satisfied that it would be contrary to the public interest for this subsection to apply to the requirement.

(114) Schedule 1, item 7, page 56 (after line 16), after subsection 317ZK(3), insert:

(3A) In deciding whether it would be contrary to the public interest for subsection (3) to apply to the requirement, the Director-General of Security, the chief officer or the Attorney-General, as the case may be, must have regard to the following matters:

(a) in the case of a requirement under a technical assistance notice given by the chief officer of an interception agency or a
requirement under a technical capability notice that relates to an interception agency—the interests of law enforcement;

(b) in the case of a requirement under a technical assistance notice given by the Director-General of Security or a requirement under a technical capability notice that relates to ASIO—the interests of national security;

(c) the objects of this Act;

(d) the extent to which compliance with the requirement will impose a regulatory burden on the provider;

(e) the reasons for the giving of the technical assistance notice or technical capability notice, as the case requires;

(f) such other matters (if any) as the Director-General of Security, the chief officer or the Attorney-General, as the case may be, considers relevant.

[terms and conditions on which help is to be given]

(115) Schedule 1, item 7, page 57 (after line 2), after subsection 317ZK(6), insert:

(6A) Subsection (4) does not apply to the requirement if:

(a) in the case of a requirement under a technical assistance notice given by the Director-General of Security—the Director-General of Security declares in writing that the Director-General of Security is satisfied that it would be contrary to the public interest for subsection (4) to apply to the requirement; or

(b) in the case of a requirement under a technical assistance notice given by the chief officer of an interception agency—the chief officer declares in writing that the chief officer is satisfied that it would be contrary to the public interest for subsection (4) to apply to the requirement; or

(c) in the case of a requirement under a technical capability notice—the Attorney-General declares in writing that the Attorney-General is satisfied that it would be contrary to the public interest for subsection (4) to apply to the requirement.

(6B) In deciding whether it would be contrary to the public interest for subsection (4) to apply to the requirement, the Director-General of Security, the chief officer or the Attorney-General, as the case may be, must have regard to the following matters:

(a) in the case of a requirement under a technical assistance notice given by the chief officer of an interception agency or a requirement under a technical capability notice that relates to an interception agency—the interests of law enforcement;

(b) in the case of a requirement under a technical assistance notice given by the Director-General of Security or a requirement under
a technical capability notice that relates to ASIO—the interests of national security;
(c) the objects of this Act;
(d) the extent to which compliance with the requirement will impose a regulatory burden on the provider;
(e) the reasons for the giving of the technical assistance notice or technical capability notice, as the case requires;
(f) such other matters (if any) as the Director-General of Security, the chief officer or the Attorney-General, as the case may be, considers relevant.

[terms and conditions on which help is to be given]

(116) Schedule 1, item 7, page 57 (line 8), before “Minister”, insert “Home Affairs”.

[Home Affairs Minister]

(117) Schedule 1, item 7, page 57 (line 14), before “Minister”, insert “Home Affairs”.

[Home Affairs Minister]

(118) Schedule 1, item 7, page 57 (line 17), before “Minister”, insert “Home Affairs”.

[Home Affairs Minister]

(119) Schedule 1, item 7, page 57 (line 21), before “Minister”, insert “Home Affairs”.

[Home Affairs Minister]

(120) Schedule 1, item 7, page 58 (after line 10), at the end of section 317ZK, add:

Technical capability notice that relates to ASIO

(17) For the purposes of this section, a technical capability notice relates to ASIO if the acts or things specified in the notice:
   (a) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or
   (b) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b).

Technical capability notice that relates to an interception agency

(18) For the purposes of this section, a technical capability notice relates to an interception agency if the acts or things specified in the notice:
(a) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to the interception agency in relation to a matter covered by paragraph 317T(2)(a); or
(b) are by way of giving help to the interception agency in relation to a matter covered by paragraph 317T(2)(b).

Technical assistance notice information

(19) For the purposes of this Part, information about a declaration under:

(a) paragraph (1)(c); or
(b) paragraph (1)(d); or
(c) paragraph (3)(d); or
(d) paragraph (3)(e); or
(e) paragraph (6A)(a); or
(f) paragraph (6A)(b);

is taken to be information about a technical assistance notice.

Technical capability notice information

(20) For the purposes of this Part, information about a declaration under paragraph (1)(e), (3)(f) or (6A)(c) is taken to be information about a technical capability notice.

[terms and conditions on which help is to be given]

(121) Schedule 1, item 7, page 58 (before line 11), before section 317ZL, insert:

317ZKA Notification obligations

(1) If the Director-General of Security makes a declaration under paragraph 317ZK(1)(c), (3)(d) or (6A)(a), the Director-General of Security must, within 7 days after making the declaration, notify the Inspector-General of Intelligence and Security of the making of the declaration.

(2) If the chief officer of an interception agency makes a declaration under paragraph 317ZK(1)(d), (3)(e) or (6A)(b), the chief officer must, within 7 days after making the declaration, notify the Commonwealth Ombudsman of the making of the declaration.

(3) If:

(a) the Attorney-General makes a declaration under paragraph 317ZK(1)(e), (3)(f) or (6A)(c) in relation to a technical capability notice; and
(b) the acts or things specified in the notice:
are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to ASIO in relation to a matter covered by paragraph 317T(2)(a); or

(ii) are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b);

the Attorney-General must, within 7 days after making the declaration, notify the Inspector-General of Intelligence and Security of the making of the declaration.

(4) If:

(a) the Attorney-General makes a declaration under paragraph 317K(1)(e), (3)(f) or (6A)(c) in relation to a technical capability notice; and

(b) the acts or things specified in the notice:

(i) are directed towards ensuring that a designated communications provider is capable of giving listed help (within the meaning of section 317T) to an interception agency in relation to a matter covered by paragraph 317T(2)(a); or

(ii) are by way of giving help to an interception agency in relation to a matter covered by paragraph 317T(2)(b);

the Attorney-General must, within 7 days after making the declaration, notify the Commonwealth Ombudsman of the making of the declaration.

(5) A failure to comply with subsection (1), (2), (3) or (4) does not affect the validity of a declaration under:

(a) paragraph 317ZK(1)(c); or

(b) paragraph 317ZK(1)(d); or

(c) paragraph 317ZK(1)(e); or

(d) paragraph 317ZK(3)(d); or

(e) paragraph 317ZK(3)(e); or

(f) paragraph 317ZK(3)(f); or

(g) paragraph 317ZK(6A)(a); or

(h) paragraph 317ZK(6A)(b); or

(i) paragraph 317ZK(6A)(c).

[notification obligations]

(122) Schedule 1, item 7, pages 60 and 61 (table item 2), omit the table item.

[interception agency—chief officer and officer]

(123) Schedule 1, item 7, page 61 (table item 5), omit the table item.

[interception agency—chief officer and officer]
(124) Schedule 1, item 7, pages 61 and 62 (table item 6), omit the table item.

[interception agency—chief officer and officer]

(125) Schedule 1, item 7, page 62 (table item 7), omit the table item.

[interception agency—chief officer and officer]

(126) Schedule 1, item 7, page 62 (table item 8), omit the table item.

[interception agency—chief officer and officer]

(127) Schedule 1, item 7, pages 62 and 63 (table item 9), omit the table item.

[interception agency—chief officer and officer]

(128) Schedule 1, item 7, page 63 (table item 10), omit the table item.

[interception agency—chief officer and officer]

(129) Schedule 1, item 7, page 63 (table item 11), omit the table item.

[interception agency—chief officer and officer]

(130) Schedule 1, item 7, page 65 (table item 2), omit the table item.

[delegation by chief officer of an interception agency]

(131) Schedule 1, item 7, page 65 (table item 5), omit the table item.

[delegation by chief officer of an interception agency]

(132) Schedule 1, item 7, page 65 (table item 6), omit the table item.

[delegation by chief officer of an interception agency]

(133) Schedule 1, item 7, pages 65 and 66 (table item 7), omit the table item.

[delegation by chief officer of an interception agency]

(134) Schedule 1, item 7, page 66 (table item 8), omit the table item.

[delegation by chief officer of an interception agency]

(135) Schedule 1, item 7, page 66 (table item 9), omit the table item.

[delegation by chief officer of an interception agency]

(136) Schedule 1, item 7, page 66 (table item 10), omit the table item.

[delegation by chief officer of an interception agency]

(137) Schedule 1, item 7, page 67 (after line 7), after section 317ZR, insert:
317ZRA Relationship of this Part to parliamentary privileges and immunities

To avoid doubt, this Part does not affect the law relating to the powers, privileges and immunities of any of the following:

(a) each House of the Parliament;
(b) the members of each House of the Parliament;
(c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

[parliamentary privileges and immunities]

(138) Schedule 1, item 7, page 67 (before line 8), before section 317ZS, insert:

317ZRB Inspection of records

(1) An Ombudsman official may inspect the records of an interception agency to determine the extent of compliance with this Part by:

(a) the agency; and
(b) the chief officer of the agency; and
(c) officers of the agency.

(2) The chief officer of an interception agency must ensure that officers of the agency give an Ombudsman official any assistance the Ombudsman official reasonably requires to enable the Ombudsman official to exercise the power conferred by subsection (1).

Report

(3) The Commonwealth Ombudsman may make a written report to the Home Affairs Minister on the results of one or more inspections under subsection (1).

(4) A report under subsection (3) must not include information which, if made public, could reasonably be expected to:

(a) prejudice an investigation or prosecution; or
(b) compromise any interception agency’s operational activities or methodologies.

(5) If:

(a) the Commonwealth Ombudsman makes a report under subsection (3); and
(b) the report relates to an inspection under subsection (1) of the records of an interception agency of a State or Territory;
the Commonwealth Ombudsman must give a copy of the report to the chief officer of the interception agency.
(6) If the Home Affairs Minister receives a report under subsection (3), the Home Affairs Minister must cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Home Affairs Minister receives the report.

(7) Before tabling the copy of the report, the Home Affairs Minister may delete from the copy information that, if made public, could reasonably be expected to:
   (a) prejudice an investigation or prosecution; or
   (b) compromise any interception agency’s operational activities or methodologies.

(139) Schedule 1, item 7, page 67 (line 9), before “Minister”, insert “Home Affairs”.

(140) Schedule 1, item 7, page 67 (line 21), at the end of subsection 317ZS(1), add:
; and (d) if any technical assistance requests, technical assistance notices or technical capability notices given during the year ending on that 30 June related to the enforcement of the criminal law so far as it relates to one or more kinds of serious Australian offences—those kinds of serious Australian offences.

(141) Schedule 1, page 67 (after line 32), after item 7, insert:

**7A After paragraph 570(3)(a)**

Insert:

(aa) in the case of a contravention of subsection 317ZA(1) or (2)—47,619 penalty units for each contravention; or

**7B After subsection 570(4B)**

Insert:

(4C) Subsection (4) does not apply to a contravention of subsection 317ZA(1) or (2).

(4D) The pecuniary penalty payable under subsection (1) by a person other than a body corporate for a contravention of subsection 317ZA(1) or (2) is not to exceed 238 penalty units for each contravention.

(142) Schedule 1, page 68 (before line 1), before the heading, insert:
Telecommunications (Interception and Access) Act 1979

7C At the end of section 83
Add:

(4) If:

(a) the performance of a function, or the exercise of a power, conferred by Part 15 of the Telecommunications Act 1997 is in connection with an interception warrant; and

(b) a Commonwealth agency has records that relate to the performance of that function or the exercise of that power;

the Ombudsman may inspect those records in order to ascertain the extent to which the agency’s officers have complied with Part 15 of the Telecommunications Act 1997.

[inspection of records]

(143) Schedule 1, page 68, after proposed item 7C, insert:

7D Subsection 84(1)
Omit “and (3)”, substitute “, (3) and (4)”.

[inspection of records]

(144) Schedule 1, page 68, after proposed item 7D, insert:

7E After subsection 186B(1)
Insert:

(1A) If:

(a) the performance of a function, or the exercise of a power, conferred by Part 15 of the Telecommunications Act 1997 is in connection with:

(i) a stored communications warrant; or
(ii) an authorisation under Division 3, 4 or 4A of Part 4-1; and

(b) an enforcement agency has records that relate to the performance of that function or the exercise of that power;

the Ombudsman may inspect those records in order to determine the extent of compliance with Part 15 of the Telecommunications Act 1997 by the agency and its officers.

[inspection of records]

(145) Schedule 1, page 68, after proposed item 7E, insert:
7F Section 187N (heading)
Omit “Part”, substitute “this Part and the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018”.

7G Subsection 187N(1)
After “this Part”, insert “and the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018”.

[review]

(146) Schedule 2, page 70 (after line 8), after item 6, insert:

6A After subsection 25A(4)
Insert:

(4A) If:
(a) the warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph (4)(ac); and
(b) a computer or thing is removed from the premises in accordance with the warrant;
the computer or thing must be returned to the premises:
(c) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or
(d) otherwise—within a reasonable period.

[computer access warrant—return of computer or other thing]

(147) Schedule 2, item 7, page 71 (after line 11), after subsection 25A(8), insert:

(9) Subsection (8) does not authorise the doing of a thing that is likely to:
(a) materially interfere with, interrupt or obstruct:
   (i) a communication in transit; or
   (ii) the lawful use by other persons of a computer;
   unless the doing of the thing is necessary to do one or more of the things specified in subsection (8); or
(b) cause any other material loss or damage to other persons lawfully using a computer.

(10) If a computer or another thing is removed from a place in accordance with paragraph (8)(f), the computer or thing must be returned to that place:
(a) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or
(b) otherwise—within a reasonable period.

[computer access warrant—concealment of access]

(148) Schedule 2, item 8, page 72 (after line 14), after subsection 27A(3C), insert:

(3D) Subsection (3C) does not authorise the doing of a thing that is likely to:
(a) materially interfere with, interrupt or obstruct:
   (i) a communication in transit; or
   (ii) the lawful use by other persons of a computer;
   unless the doing of the thing is necessary to do one or more of the things specified in subsection (3C); or
(b) cause any other material loss or damage to other persons lawfully using a computer.

(3E) If a computer or another thing is removed from a place in accordance with paragraph (3C)(f), the computer or thing must be returned to that place:
(a) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or
(b) otherwise—within a reasonable period.

[foreign intelligence warrant—concealment of access]

(149) Schedule 2, page 72 (after line 34), after item 11, insert:

11A After subsection 27E(3)

   Insert:

   Return of computer or other thing

   (3A) If:
      (a) an authorisation under subsection (2) authorises the removal of a computer or other thing from premises as mentioned in paragraph (2)(da); and
      (b) a computer or thing is removed from the premises in accordance with the authorisation;
   the computer or thing must be returned to the premises:
      (c) if returning the computer or thing would be prejudicial to security—when returning the computer or thing would no longer be prejudicial to security; or
      (d) otherwise—within a reasonable period.
(150) Schedule 2, item 12, page 74 (after line 2), after subsection 27E(6), insert:

(7) Subsection (6) does not authorise the doing of a thing that is likely to:
   (a) materially interfere with, interrupt or obstruct:
       (i) a communication in transit; or
       (ii) the lawful use by other persons of a computer;
       unless the doing of the thing is necessary to do one or more of the
       things specified in subsection (6); or
   (b) cause any other material loss or damage to other persons lawfully
       using a computer.

(8) If a computer or another thing is removed from a place in accordance
with paragraph (6)(f), the computer or thing must be returned to the
place:
   (a) if returning the computer or thing would be prejudicial to
       security—when returning the computer or thing would no longer
       be prejudicial to security; or
   (b) otherwise—within a reasonable period.

(151) Schedule 2, page 74 (after line 4), after item 13, insert:

13A Section 34 (at the end of the heading)
Add “—general”.

[report to Attorney-General]

(152) Schedule 2, page 74 (after line 19), after item 16, insert:

16A After section 34
Insert:

34A Director-General to report to Attorney-General—concealment of
access
(1) If:
   (a) a warrant issued under this Division has ceased to be in force;
and
   (b) during a prescribed post-cessation period of the warrant, a thing
       was done under subsection 25A(8), 27A(3C) or 27E(6) in
       connection with the warrant; and
   (c) the thing has not been dealt with in a report under
       subsection 34(1);
the Director-General must:
(d) give the Attorney-General a written report on the extent to which doing the thing has assisted the Organisation in carrying out its functions; and
(e) do so as soon as practicable after the end of that period.

(2) If:
(a) a warrant issued under this Division has ceased to be in force; and
(b) as at the end of a prescribed post-cessation period of the warrant, it is likely that a thing will be done under subsection 25A(8), 27A(3C) or 27E(6) in connection with the warrant;
the Director-General must:
(c) give the Attorney-General a written report on the extent to which doing the thing will assist the Organisation in carrying out its functions; and
(d) do so as soon as practicable after the end of that period.

Prescribed post-cessation period

(3) For the purposes of this section, each of the following periods is a prescribed post-cessation period of a warrant:
(a) the 3-month period beginning immediately after the warrant ceased to be in force;
(b) each subsequent 3-month period.

[report to Attorney-General]

(153) Schedule 2, item 49, page 89 (line 35), at the end of paragraph 27D(1)(b), add:
; and (xii) any conditions subject to which things may be done under the warrant.

[computer access warrants—conditions]

(154) Schedule 2, item 49, page 92 (after line 8), after subsection 27E(2), insert:

(2A) If:
(a) a computer access warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph (2)(f); and
(b) a computer or thing is removed from the premises in accordance with the warrant;
the computer or thing must be returned to the premises within a reasonable period.

[computer access warrant—return of computer or other thing]
(155) Schedule 2, item 49, page 94 (after line 16), at the end of section 27E, add:

(8) Subsection (7) does not authorise the doing of a thing that is likely to:
   (a) materially interfere with, interrupt or obstruct:
       (i) a communication in transit; or
       (ii) the lawful use by other persons of a computer;
       unless the doing of the thing is necessary to do one or more of the
       things specified in subsection (7); or
   (b) cause any other material loss or damage to other persons lawfully
       using a computer.

(9) If a computer or another thing is removed from a place in accordance
    with paragraph (7)(f), the computer or thing must be returned to the
    place within a reasonable period.

(156) Schedule 2, item 49, page 99 (after line 23), after section 27H, insert:

27J Relationship of this Division to parliamentary privileges and immunities

To avoid doubt, this Division does not affect the law relating to the
powers, privileges and immunities of any of the following:
   (a) each House of the Parliament;
   (b) the members of each House of the Parliament;
   (c) the committees of each House of the Parliament and joint
       committees of both Houses of the Parliament.

(157) Schedule 2, page 102 (after line 26), after item 60, insert:

60A Subsection 32(4)

After “this Part”, insert “(other than subsection (2A) of this section)”.

(158) Schedule 2, page 118 (after line 28), after item 104, insert:

104A After section 49A

Insert:

49B Notification to Ombudsman in relation to concealment of access
under a computer access warrant

If:
(a) a computer access warrant was issued in response to an application made by a law enforcement officer of a law enforcement agency; and
(b) a thing mentioned in subsection 27E(7) was done under the warrant after the 28-day period mentioned in paragraph 27E(7)(j);
the chief officer of the law enforcement agency must:
(c) notify the Ombudsman:
   (i) that the warrant was issued; and
   (ii) of the fact that the thing was done under the warrant after the 28-day period mentioned in paragraph 27E(7)(j); and
(d) do so within 7 days after the thing was done.

[notification to Ombudsman]

(159) Schedule 2, page 121 (after line 29), after item 111, insert:

111A After subsection 55(2A)

   Insert:

(2B) If:

   (a) the performance of a function, or the exercise of a power, conferred by Part 15 of the *Telecommunications Act 1997* is in connection with a warrant; and
   (b) a law enforcement agency has records that relate to the performance of that function or the exercise of that power;
the Ombudsman may inspect those records in order to determine the extent of compliance with Part 15 of the *Telecommunications Act 1997* by the agency and law enforcement officers of the agency.

[inspection of records]

(160) Schedule 2, page 122 (after line 9), after item 113, insert:

113A Section 64

Before “If:”, insert “(1)”.

113B At the end of section 64

Add:

(2) If:

   (a) a person suffers loss or injury as a result of the use of:
   (i) a computer; or
   (ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
(iii) any other electronic equipment; or
(iv) a data storage device;
for the purpose of obtaining access to data that is held in the computer; and
(b) the use of the computer, facility, equipment or device, as the case may be, was by any of the following:
   (i) the Australian Federal Police;
   (ii) the Integrity Commissioner or a staff member of ACLEI;
   (iii) the Australian Crime Commission; and
(c) the use of the computer, facility, equipment or device, as the case may be, is prohibited by the law of the State or Territory in which the use occurs; and
(d) the use of the computer, facility, equipment or device, as the case may be, is neither:
   (i) in accordance with this Act; nor
   (ii) in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth;
the Commonwealth is liable to pay to the person who has suffered the loss or injury:
(e) such compensation as is agreed on between the Commonwealth and that person; or
(f) in default of such an agreement—such compensation as is determined by action against the Commonwealth in a court of a State or Territory that has jurisdiction in relation to the matter.

[compensation]

(161) Schedule 2, item 120, page 130 (after line 24), after the definition of *general computer access warrant*, insert:

  *Ombudsman official* means:
  (a) the Ombudsman; or
  (b) a Deputy Commonwealth Ombudsman; or
  (c) a person who is a member of the staff referred to in subsection 31(1) of the *Ombudsman Act 1976*.

  [Ombudsman official]

(162) Schedule 2, item 124, page 133 (line 17), at the end of the heading to section 63AB, add “etc.”.

  [dealing in general computer access intercept information etc.]

(163) Schedule 2, item 124, page 134 (after line 23), at the end of section 63AB, add:
(3) A person may, in connection with:
   (a) the performance by an Ombudsman official of the Ombudsman
       official’s functions or duties; or
   (b) the exercise by an Ombudsman official of the Ombudsman
       official’s powers;
communicate to the Ombudsman official, or make use of, or make a
record of, general computer access intercept information.

(4) An Ombudsman official may, in connection with:
   (a) the performance by the Ombudsman official of the Ombudsman
       official’s functions or duties; or
   (b) the exercise by the Ombudsman official of the Ombudsman
       official’s powers;
communicate to another person, or make use of, or make a record of,
general computer access intercept information.

(5) If:
   (a) information was obtained by intercepting a communication
       passing over a telecommunications system; and
   (b) the interception was purportedly for the purposes of doing a thing
       specified in a general computer access warrant; and
   (c) the interception was not authorised by the general computer
       access warrant;
then:
   (d) a person may, in connection with:
       (i) the performance by an Ombudsman official of the
           Ombudsman official’s functions or duties; or
       (ii) the exercise by an Ombudsman official of the Ombudsman
           official’s powers;
communicate to the Ombudsman official, or make use of, or
make a record of, that information; and
   (e) an Ombudsman official may, in connection with:
       (i) the performance by the Ombudsman official of the
           Ombudsman official’s functions or duties; or
       (ii) the exercise by the Ombudsman official of the Ombudsman
           official’s powers;
communicate to another person, or make use of, or make a record
of, that information.

(6) Despite subsection 13.3(3) of the Criminal Code, in a prosecution for
an offence against section 63 of this Act, an Ombudsman official does
not bear an evidential burden in relation to the matters in subsection (4)
or (5) of this section.

[dealing in general computer access intercept information etc.]
(164) Schedule 2, item 124, page 134 (line 24), at the end of the heading to section 63AC, add “etc.”.

[dealing in ASIO computer access intercept information etc.]

(165) Schedule 2, item 124, page 135 (after line 24), at the end of section 63AC, add:

(3) A person may, in connection with:
   (a) the performance by an IGIS official of the IGIS official’s functions or duties; or
   (b) the exercise by an IGIS official of the IGIS official’s powers;
communicate to the IGIS official, or make use of, or make a record of, ASIO computer access intercept information.

(4) An IGIS official may, in connection with:
   (a) the performance by the IGIS official of the IGIS official’s functions or duties; or
   (b) the exercise by the IGIS official of the IGIS official’s powers;
communicate to another person, or make use of, or make a record of, ASIO computer access intercept information.

(5) If:
   (a) information was obtained by intercepting a communication passing over a telecommunications system; and
   (b) the interception was purportedly for the purposes of doing a thing specified in an ASIO computer access warrant; and
   (c) the interception was not authorised by the ASIO computer access warrant;
then:
   (d) a person may, in connection with:
      (i) the performance by an IGIS official of the IGIS official’s functions or duties; or
      (ii) the exercise by an IGIS official of the IGIS official’s powers;
communicate to the IGIS official, or make use of, or make a record of, that information; and
   (e) an IGIS official may, in connection with:
      (i) the performance by the IGIS official of the IGIS official’s functions or duties; or
      (ii) the exercise by the IGIS official of the IGIS official’s powers;
communicate to another person, or make use of, or make a record of, that information.
Despite subsection 13.3(3) of the Criminal Code, in a prosecution for an offence against section 63 of this Act, an IGIS official does not bear an evidential burden in relation to the matters in subsection (4) or (5) of this section.

[dealing in ASIO computer access intercept information etc.]

(166) Schedule 3, page 154 (after line 16), after item 10, insert:

10A At the end of Division 2 of Part IAA

Add:

3SA Relationship of this Division to parliamentary privileges and immunities

To avoid doubt, this Division does not affect the law relating to the powers, privileges and immunities of any of the following:

(a) each House of the Parliament;
(b) the members of each House of the Parliament;
(c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

[parliamentary privileges and immunities]

(167) Schedule 4, page 166 (after line 2), after item 18D, insert:

18E At the end of Subdivision C of Division 1 of Part XII

Add:

202B Relationship of this Subdivision to parliamentary privileges and immunities

To avoid doubt, this Subdivision does not affect the law relating to the powers, privileges and immunities of any of the following:

(a) each House of the Parliament;
(b) the members of each House of the Parliament;
(c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

[parliamentary privileges and immunities]

(168) Schedule 5, item 2, page 167 (line 30) to page 168 (line 1), omit subsection 21A(2), substitute:

(2) A request under paragraph (1)(a) may be made orally if:
(a) the Director-General is satisfied that the request should be made as a matter of urgency; or
(b) the Director-General is satisfied that making the request in writing would be prejudicial to security; or
(c) the Director-General is satisfied that making the request in writing would be prejudicial to the operational security of the Organisation.

(2A) If subsection (2) does not apply to a request under paragraph (1)(a), the request must be made in writing.

[voluntary assistance requests]

(169) Schedule 5, item 2, page 168 (after line 5), after subsection 21A(3), insert:

(3A) If a request is made under paragraph (1)(a), the Director-General must, within 7 days after the request is made, notify the Inspector-General of Intelligence and Security that the request has been made.

[notification to Inspector-General of Intelligence and Security]

(170) Schedule 5, page 169 (after line 25), after item 2, insert:

2A After subsection 34(1)

Insert:

(1A) If an order was made under subsection 34AAA(2) in relation to the warrant, the report must also include details of the extent to which compliance with the order has assisted the Organisation in carrying out its functions.

[report to Attorney-General]

(171) Schedule 5, item 3, page 172 (after line 27), after subsection 34AAA(3), insert:

(3A) A request under subsection (1) may be made:
   (a) orally; or
   (b) in writing.

(3B) If a request under subsection (1) is made orally, the Director-General must:
   (a) make a written record of the request; and
   (b) do so within 48 hours after the request was made.

(3C) A request under subsection (1) (the current request) must be accompanied by a statement setting out the particulars and outcomes of all previous requests (if any) under that subsection for the making of an order relating to the person specified in the current request.
(3D) If the Director-General is satisfied that the grounds on which an order under this section was made have ceased to exist, the Director-General must, as soon as practicable, inform the Attorney-General of that fact.

(3E) If:
   (a) an order is in force under this section; and
   (b) the Attorney-General is satisfied that the grounds on which the order was made have ceased to exist;
   the Attorney-General must revoke the order.

[assistance relating to access to data]

(172) Schedule 5, page 172 (after line 35), at the end of the Schedule, add:

4 Section 34ZH
   Before “The Director-General”, insert “(1)”.

5 At the end of section 34ZH
   Add:
   (2) If an order was made under subsection 34AAA(2) in relation to accessing data that was held in, or accessible from, a computer or storage device that was seized under section 34ZB, the report must also include details of the extent to which compliance with the order has assisted the Organisation in carrying out its functions.

[report to Attorney-General]
Schedule 5, page 172, at the end of the Schedule, add (after proposed item 5):

6 Before subsection 94(2C)

Insert:

(2BC) A report under subsection (1) must also include a statement of:
   (a) the total number of requests made under paragraph 21A(1)(a)
       during the period; and
   (b) the total number of orders made under subsection 34AAA(2)
       during the period.

[annual report]

DAVID ELDER
Clerk of the House of Representatives

House of Representatives
6 December 2018