

2016 – 2017 – 2018

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

**TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT
(ASSISTANCE AND ACCESS) BILL 2018**

SUPPLEMENTARY EXPLANATORY MEMORANDUM

Amendments to be Moved on Behalf of the Government

(Circulated by authority of the Attorney-General, the Honourable Christian Porter MP, for the
Minister for Home Affairs, the Honourable Peter Dutton MP)

TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) BILL 2018

GENERAL OUTLINE

The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 amends the *Telecommunications Act 1997* (Telecommunications Act), the *Telecommunications (Interception and Access) Act 1979*, and related legislation, including the *Surveillance Devices Act 2004*, the *Crimes Act 1914*, the *Mutual Assistance in Criminal Matters Act 1987*, the *Australian Security Intelligence Organisation Act 1979* and the *Customs Act 1901*, to introduce measures to better deal with the challenges posed by ubiquitous encryption.

The amendments to the Bill will:

- enhance existing oversight arrangements for agencies and provide review mechanisms—namely legislative review by the Independent National Security Legislation Monitor within 18 months of commencement, and review by the Parliamentary Joint Committee on Intelligence and Security in early 2019
- provide for explicit inspection powers of Schedule 1 measures by the Commonwealth Ombudsman and enhancing the ability of the Ombudsman to inspect the exercise of these powers in conjunction with underlying interception and surveillance device warrants
- add to reporting requirements on the use of Schedule 1 and Schedule 5 powers
- ensure the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman are notified of the issue, variation, extension and revocation of all industry assistance measures
- define ‘systemic weakness’ and ‘systemic vulnerability’ to enable technical reporting to assist in whether a technical capability notice would breach the legislative limitations, and applying this definition more broadly to Schedule 1
- enhance the protections against systemic weakness and vulnerability by making clear that industry assistance cannot be requested or required if it would, or would be likely, to jeopardise the security of any information held by a person other than a person connected with a target technology, including if the act or thing or requested or required would create a material risk that otherwise secure information can be accessed by an unauthorised third party
- enhance the independent assessment (on referral) of whether requirements to build a new capability create a systemic weakness and are reasonable, proportionate, practicable and technically feasible
- extend decision-making requirements and the limitation against building or implementing systemic weaknesses to voluntary measures in Schedule 1
- narrow the functions for which intelligence agencies can seek voluntary assistance

- limit the application of the industry assistance measures to the investigation and prosecution of serious offences (offences with a maximum period of imprisonment of 3 years' or more)
- make the activities that may be required by a notice in Schedule 1 exhaustive and clarify that they can be used to facilitate or assist in giving effect to warrants and authorisations
- ensure decision-makers consider the necessity of measures under Schedule 1 and that any conduct would be the least intrusive to third parties
- impose time-limits of 12 months for technical assistance notices and technical capability notices
- allow for 'designated communications providers' to disclose information about a technical capability notice with agreement from the relevant agency and subject to conditions
- clarify that disclosures can be made between law enforcement agencies and oversight bodies for Schedules 1 and 2
- clarify the appropriate civil penalties in line with other similar assistance obligations under the Telecommunications Act
- clarify that for the purposes of Part 15 of the Telecommunications Act a reference to 'Minister' is a reference to the Minister for Home Affairs
- provide for Commonwealth scrutiny of technical assistance notices by the chief officer of an interception agency of a State or Territory
- allow designated communication providers to refer technical capability notices to the Attorney-General for review to determine if the notice creates a systemic weakness
- limit the definition of 'interception agency' to Commonwealth, State and Territory police
- require double-lock approval of technical capability notices by both the Attorney-General and the Minister for Communications
- limit the circumstances in which a technical capability notice may be varied and require approval of both the Attorney-General and the Minister
- ensure that 'ASIO computer access intercept information' and 'general computer access intercept information' is subject to restrictions on use, disclosure and requirements which relate to destruction
- allow for notification on concealment activities for ASIO and law enforcement computer access warrants, and
- place further safeguards on the exercise of compulsory powers in Schedule 5.

ABBREVIATIONS

The following abbreviations will be incorporated throughout this supplementary explanatory memorandum:

- Administrative Appeals Tribunal (AAT)
- *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act)
- Australian Border Force (ABF)
- Australian Federal Police (AFP)
- Australian Geospatial Organisation (AGO)
- Australian Signals Directorate (ASD)
- Australian Security Intelligence Organisation (ASIO)
- *Australian Security Intelligence Organisation Act 1979* (ASIO Act)
- Australian Secret Intelligence Service (ASIS)
- *Criminal Code Act 1995* (Criminal Code)
- *Crimes Act 1914* (Crimes Act)
- *Customs Act 1901* (Customs Act)
- Independent National Security Legislation Monitor (INSLM)
- *Independent National Security Legislation Monitor Act 2010* (INSLM Act)
- Inspector-General of Intelligence and Security (IGIS)
- *Inspector-General of Intelligence and Security Act 1986* (IGIS Act)
- *Intelligence Services Act 2001* (IS Act)
- *Mutual Assistance in Criminal Matters Act 1987* (MACMA)
- *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act)
- *Surveillance Devices Act 2004* (SD Act)
- *Telecommunications Act 1997* (Telecommunications Act)
- *Telecommunications (Interception and Access) Act 1979* (TIA Act)
- Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2017 (Bill)
- Voice over Internet Protocol (VoIP)

FINANCIAL IMPACT

Financial impacts will be met from existing appropriations.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

AMENDMENTS TO THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) BILL 2018

1. These amendments are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the amendments to the Bill

2. The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Bill) will amend the *Telecommunications Act 1997* (Telecommunications Act) and related legislation, including the *Telecommunications (Interception and Access) Act 1979* (TIA Act), *Surveillance Devices Act 2004* (SD Act), the *Crimes Act 1914* (Crimes Act), the *Mutual Assistance in Criminal Matters Act 1987* (MACMA), the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Customs Act 1901* (Customs Act), to assist agencies to adapt to an operating environment characterised by ubiquitous encryption.

3. The amendments to the Bill will:

- enhance existing oversight arrangements for agencies and provide review mechanisms—namely legislative review by the Independent National Security Legislation Monitor within 18 months of commencement, and review by the Parliamentary Joint Committee on Intelligence and Security in early 2019
- provide for explicit inspection powers of Schedule 1 measures by the Commonwealth Ombudsman and enhancing the ability of the Ombudsman to inspect the exercise of these powers in conjunction with underlying interception and surveillance device warrants
- add to reporting requirements on the use of Schedule 1 and Schedule 5 powers
- ensure the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman are notified of the issue, variation, extension and revocation of all industry assistance measures
- define ‘systemic weakness’ and ‘systemic vulnerability’ to enable technical reporting to assist in whether a technical capability notice would breach the legislative limitations, and applying this definition more broadly to Schedule 1
- enhance the independent assessment (on referral) of whether requirements to build a new capability create a systemic weakness and are reasonable, proportionate, practicable and technically feasible
- extend decision-making requirements and the limitation against building or implementing systemic weaknesses to voluntary measures in Schedule 1
- narrow the functions for which intelligence agencies can seek voluntary assistance

- limit the application of the industry assistance measures to the investigation and prosecution of serious offences (offences with a maximum period of imprisonment of 3 years' or more)
- make the activities that may be required by a notice in Schedule 1 exhaustive and clarify that they can be used to facilitate or assist in giving effect to warrants and authorisations
- ensure decision-makers consider the necessity of measures under Schedule 1 and that any conduct would be the least intrusive to third parties
- impose time-limits of 12 months for technical assistance notices and technical capability notices
- allow for 'designated communications providers' to disclose information about a technical capability notice with agreement from the relevant agency and subject to conditions
- clarify that disclosures can be made between law enforcement agencies and oversight bodies for Schedules 1 and 2
- clarify the appropriate civil penalties in line with other similar assistance obligations under the Telecommunications Act
- clarify that for the purposes of Part 15 of the Telecommunications Act a reference to 'Minister' is a reference to the Minister for Home Affairs
- provide for Commonwealth scrutiny of technical assistance notices by the chief officer of an interception agency of a State or Territory
- allow designated communication providers to refer technical capability notices to the Attorney-General for review to determine if the notice creates a systemic weakness
- limit the definition of 'interception agency' to Commonwealth, State and Territory police
- require double-lock approval of technical capability notices by both the Attorney-General and the Minister for Communications
- limit the circumstances in which a technical capability notice may be varied and require approval of both the Attorney-General and the Minister
- ensure that 'ASIO computer access intercept information' and 'general computer access intercept information' is subject to restrictions on use, disclosure and requirements which relate to destruction
- allow for notification on concealment activities for ASIO and law enforcement computer access warrants, and
- place further safeguards on the exercise of compulsory powers in Schedule 5.

Human rights implications

4. The amendments are consistent with Australia's human rights obligations and engage the following human right, which was identified in the Statement of Compatibility in the Explanatory Memorandum to the Bill, as introduced and read for a second time in the House of Representatives on 20 September 2018:

- protection against arbitrary or unlawful interference with privacy contained in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)

Human rights impacted by the Government amendments

Protection against arbitrary or unlawful interference with privacy – Article 17 of the ICCPR

5. Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation, and that everyone has the right to the protection of the law against such interference or attacks.

6. The right to privacy under Article 17 can be permissibly limited in order to achieve a legitimate objective and where the limitations are lawful and not arbitrary. The term 'unlawful' in Article 17 of the ICCPR means that no interference can take place except as authorised under domestic law. Additionally, the term 'arbitrary' in Article 17(1) of the ICCPR means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances.¹ The United Nations Human Rights Committee has interpreted 'reasonableness' to mean that any limitation must be proportionate and necessary in the circumstances.

7. Amendments have been made to the Bill to strengthen existing limitations, which ensures key measures do not arbitrarily or unlawfully interfere with the right to privacy, while equipping law enforcement and national security agencies with the tools to investigate and prosecute serious criminals and terrorists. These amendments, which relate to Article 17 of the ICCPR, include:

- Introducing additional definitions for 'serious Australian offence' and 'serious foreign offence' for the purposes of Part 15 of the Telecommunications Act concerning industry assistance (section 317B) to ensure the powers set out in Schedule 1 of the Bill can only be used 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, or for life. These definitions further clarify that the exercise of powers in Schedule 1 are a permissible limitation to the right to privacy as they are reserved for serious offences including terrorism and child exploitation offences. Invoking the powers in Schedule 1 is a reasonable and proportionate interference with the right to privacy given the nature of the offences under investigation.
- Requiring decision-makers under the Telecommunications Act to consider if the requirements under a technical assistance notice or technical capability notice are the least intrusive known form of industry assistance when compared to other forms of

¹ *Toonen v Australia*, Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994) at 8.3.

industry assistance in relation to the impact on the privacy of innocent third parties (sections 317JC for technical assistance requests, 317RA for technical assistance notices and new section 317ZAA for technical capability notices). This requirement to assess whether the proposed requirements are the least intrusive further limits the ability of Schedule 1 powers being used to arbitrarily or unlawfully interfere with the privacy of innocent parties.

- Section 317P of the Telecommunications Act ensures that technical capability notices can only be issued if the decision-maker is satisfied that the requirements in the notice are reasonable and proportionate. Section 317V in the Bill ensures that technical capability notices can only be issued if the Attorney-General is satisfied that the requirements in a notice are reasonable and proportionate, and that compliance with a notice is practicable and technically feasible.

The amendments include considerations of necessity in new sections 317JAA, 317RA and 317ZAA of the Telecommunications Act which strengthens the aforementioned decision-making criteria to ensure that decisions-makers have regard to whether a technical assistance notice or technical capability notice is necessary for achieving legitimate beneficial outcomes for law enforcement and national security.

The amendments at sections 317JAA, 317RA and 317ZAA provides confidence that, under the oversight of the decision-maker, any limitation to the right of privacy under a compulsory notice in Schedule 1 of the Bill is permissible as being necessary to ensure national security and public order.

- Imposing time-limits of 12 months for technical assistance notices and technical capability notices in new sections 317MA and 317TA in the Bill. This mandatory time-limit (extendable for a period of a further 12 months with the agreement of the provider) ensures notices are not in perpetuate existence, and that decision-makers re-evaluate the reasonableness and proportionality of a notice if it is required for more 12 months.
- Extending consultation requirements to all compulsory powers in Schedule 1. New section 317PA of the Telecommunications Act requires the decision-maker to consult with the provider prior to the issuing of a technical assistance notice. This section does not apply if the provider voluntarily notifies the relevant agency, in a form they deem to be appropriate, of their decision to waive the right to be consulted. Specifically, new section 317PA allows providers to highlight the requirements that will undermine those systems that protect the security of personal information.

The purpose of this provision is to give certainty to providers that requirements in a notice have been issued with due regard to their legitimate concerns. It also legislates the steps agencies are likely to undertake when determining the requirements in a notice, which involves direct engagement with the provider to ensure the requirements achieve agency objectives and do not adversely impact the provider and the wider community. This amendment also supports other consultative measures in the Bill including the requirement for notices to be provided in writing to the provider under new section 317M.

By giving an opportunity to raise any concerns associated with the proposed notice, this amendment ensures that the compulsory powers in Schedule 1 are not exercised

arbitrarily, and ensures that the decision-maker is made aware of, and can consider, any unintended consequences that may result from the issuing of a notice under Schedule 1.

- Amendments in section 317MAA require decision-makers to notify the provider of their right to complain about an agencies' activities to the relevant Commonwealth, State or Territory oversight body, ensuring that they have a clear avenue for redress.
- Limiting the listed act or things in new section 317E of the Bill to be exhaustive for technical assistance notices and technical capability notices. Prior to this amendment, technical assistance notices could be issued for matters that were determined by the decision-maker to meet criteria in section 317P of the Bill but were not provided for in the listed acts or things.

The types of assistance listed in section 317E are broadly cast in order to be responsive to operational needs and to reflect the rapidly changing capabilities of the communications industry. The listed acts or things are necessary to ensure agencies can continue to discharge their functions which are critical to maintaining national security and public order. This exhaustive list provides further clarity as to the situations that permit the use of Schedule 1 powers which ensures that notices are not issued arbitrarily.

Clarifying the intent, and strengthening the operation of section 317ZG

8. The amendments which support the intent of new section 317ZG of the Telecommunications Act positively engage the prohibition on arbitrary or unlawful interference with privacy under Article 17. Section 317ZG establishes an explicit prohibition against providers being required to implement or build a systemic weakness or vulnerability into a form of electronic weakness. This includes actions which would make systemic methods of authentication or encryption less effective. In other words, the amendments prevent decision-makers from issuing a technical assistance notice or technical capability notice if the requirements in the notice would contravene new section 317ZG. The provisions also ensure that decision-makers cannot issue technical assistance requests if it would contravene new section 317ZG. Furthermore, the original decision-maker does not ultimately determine if the proposed requirements to build a new capability would lead to a contravention of new section 317ZG, a robust independent assessment process can be enlivened by a provider to determine the ultimate security implications, and reasonableness, of any capability.

9. New section 317ZG limits the privacy implications of the powers in Schedule 1 by ensuring the security of third parties' communications are not impacted. Specifically, this section prevents requests and notices from being used as vehicles to introduce systemic weaknesses and vulnerabilities which can fundamentally undermine the security of networks and devices. The amendments enhance the operation of new section 317ZG by clarifying existing ambiguities associated with systemic weaknesses and vulnerabilities, and strengthens measures that prevent the undermining of those systems that protect the security of personal information. This further strengthens provisions that prevent the powers in Schedule 1 from being used to arbitrarily or unlawfully interfere with the privacy of innocent parties.

10. New section 317ZG is an important safeguard that supports Schedule 1 and ensures that the related powers reflect a permissible limitation on the right to privacy as they are a

necessary, reasonable and proportionate means of ensuring effective law enforcement and national security.

11. These amendments include:

- Introducing a definition for ‘systemic weakness’ and ‘systemic vulnerability’ in new section 317B to clarify and prohibit those proposed requirements in a technical assistance request, technical assistance notice or technical capability notice which will lead to unlawful and systemic intrusions into innocent parties’ devices. This definition makes clear that anything that weakens whole systems, and consequently puts the security of innocent users at risks, is prohibited. It clearly states a carve-out for targeted use of powers that are isolated to particular targeted devices and do not undermine system security.
- Introducing a non-exhaustive definition of ‘electronic protection’ in new section 317B to clarify those technologies which must not be undermined as they are critical to protecting the security of personal information.
- Introducing a definition of ‘target technology’ in new section 317B to clarify the targeted use of the powers.
- Introducing new section 317WA in the Telecommunications Act which establishes a framework for providers to request the carrying out of an assessment of a new capability. The independent assessors, which are appointed as per subsection 317WA(2), will consider whether requirements to build a new capability create a systemic weakness and are reasonable, proportionate, practicable and technically feasible.
- The Attorney-General must consider the report when issuing the notice. The assessors are persons eminently qualified to scrutinize the security implications of new capabilities, one being a technical expert and the other a retired senior judge.
- This is an additional safeguard to the consultation requirements under section 317W. The purpose of this amendment is to ensure providers are afforded an opportunity to challenge the requirements in a notice if they believe it may lead to the introduction of a systemic weakness or vulnerability or if the requirements are not reasonable or proportionate. This is an important measure as it ensures that the requirements in a proposed notice are altered before the notice is issued in order to prevent those systems which maintain the security of personal information from being undermined.
- Broadening the scope of new section 317ZG to include technical assistance requests. This ensures providers do not unwittingly introduce a systemic weakness or vulnerability into their networks or devices.

Enhanced approval, inspection and oversight

12. The amendments establish a process whereby technical capability notices require joint authorisation by agreement from both the Attorney-General and Minister for Communications and the Arts. This will ensure that technical capability notices will only be issued when an appropriately high level of authorisation and scrutiny has been applied to a relevant request.

13. Further, the amendments include a suite of enhanced oversight measures, including robust notification requirements and clear authority for the IGIS, Commonwealth Ombudsman and State and Territory oversight bodies to inspect and report on the use of powers under the Bill.

14. Existing reporting regimes have been augmented to allow the Commonwealth Ombudsman to further scrutinise the use of industry assistance measures in conjunction with underlying interception and surveillance powers. Further, the Bill now establishes clear channels for information exchange between oversight bodies to ensure the necessary information is available for assessing agency compliance with the law.

15. Reporting requirements have been set for powers across the Bill, including in classified ASIO annual reports that are scrutinised by Parliament and Government.

Additional protections Schedules 2 & 5

16. Additional restrictions, reporting and notification measures have been placed on the exercise of computer access powers and compulsory orders for access to data by the Director-General of ASIO. These amendments further bound the use of intrusive and covert powers and allow oversight bodies to better monitor their exercise.

Conclusion

17. The amendments are compatible with human rights because they clarify and strengthen limitations which reduce the impact to the right to privacy, and to the extent that the amendments limit the right to privacy, those limitations are necessary, reasonable and proportionate.

NOTES ON AMENDMENTS

Amendment 1

Clause 2, page 2 (table item 2)

18. This amendment substitutes item 2 of the table under subsection 2(1) of the Bill. New table item 2 provides that Part 1 of Schedule 1 to the Bill commences the day after the Act receives Royal Assent.

Amendment 2

Schedule 1, page 4 (before line 7)

19. This amendment inserts new item 1A. Item 1A inserts new subsection 94(2BA) and (2BB) after subsection 94(2B) in the ASIO Act.

20. Section 94 of the ASIO Act sets out the requirements for what must be included in the annual report prepared by the Director-General of Security and given to the Minister under section 46 of the *Public Governance, Performance and Accountability Act 2013*. A copy of the annual report must also be given to the Leader of the Opposition in the House of Representatives and, following any deletions by the Minister as provided for in subsection 94(5), laid before each House of the Parliament within 20 sitting days of that House after the report is received by the Minister.

21. New subsection 94(2BA) provides that the annual report under subsection 94(1) must also include a statement of:

- the total number of technical assistance requests given by the Director-General under paragraph 317G(1)(a) of the Telecommunications Act during the reporting period,
- the total number of technical assistance notices given by the Director-General under section 317L of the Telecommunications Act during the reporting period, and
- the total number of technical capability notices given by the Attorney-General under section 317T of the Telecommunications Act during the period that relate to the Organisation.

22. This amendment ensures that the Minister, the Leader of the Opposition and the Parliament has appropriate oversight of the number of technical assistance notices, technical assistance requests and technical capability notices issued by the Director-General of Security in a given period.

23. New subsection 94(2BB) provides that, for the purposes of new paragraph 2BA(c), a technical capability notice relates to the Organisation if the acts or things specified in the notice:

- are directed towards ensuring that a designated communications provider (within the meaning of Part 15 of the Telecommunications Act) 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
- are by way of giving help to the Organisation in relation to a matter covered by paragraph 317T(2)(b) of the Telecommunications Act.

41. This amendment provides that ‘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 or for life.

42. This amendment provides that ‘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 or for life.

Amendment 15 **Schedule 1, item 7, page 10 (after line 10)**

43. This amendment inserts a definition of ‘State and Territory inspecting authority’ after the definition of ‘staff member’ in new section 317B.

44. ‘State and 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 SD Act when the interception agency is exercising powers under the law of that State or Territory that is of a similar nature to that Act.

45. This includes oversight bodies that regularly inspect and report on the interception and surveillance activities of State and Territory police and integrity bodies, like the Office of the Inspector of the Law Enforcement Conduct Commission.

Amendment 16 **Schedule 1, item 7, page 10 (after line 19)**

46. This amendment inserts definitions of ‘systemic vulnerability’ and ‘systemic weakness’ after the definition of ‘supply’ in new section 317B.

47. ‘Systemic vulnerability’ is defined as a vulnerability that affects a whole class of technology (rather than a single item of technology), but does not include a vulnerability that is selectively introduced, on a case-by-case basis, to one or more target technologies that are connected with a particular person.

48. ‘Systemic weakness’ means a weakness that affects a whole class of technology (rather than a single item of technology), but does not include a weakness that is selectively introduced, on a case-by-case basis, to one or more target technologies that are connected with a particular person.

49. For both definitions it is immaterial whether the person can be identified. This is to account for scenarios where an underlying warrant specifies a particular Internet Protocol (IP) address or another form of particularity but a particular person cannot be identified.

50. The effect of this amendment is to clearly define the meaning of ‘systemic weakness’ and ‘systemic vulnerability’ for the purposes of the limitation on technical assistance notices, technical assistance requests and technical capability notices in new section 317ZG.

51. This definition makes clear that a systemic weakness is something that makes general items of technology less secure. Technological classes include particular mobile device models carriage services, electronic services or software. The term is intended to encompass both old and new technology or a subclass within a broader class of technology; for example an iOS mobile operating system within a particular class, or classes, of mobile devices.

Where requirements in a notice make the whole set of these items more vulnerable, it will be prohibited. This ensures that the powers do not jeopardise the general use of technology by persons who are not of interest to law enforcement and security agencies. The intent of the prohibition as expressed in the definition is to rule out requirements that would create a material risk of otherwise secure information being accessed by unauthorised third parties.

52. The definition also refines the permissible interaction with forms of electronic protection, and illustrates the targeted, selective use of the powers. It is not a systemic weakness or vulnerability if requirements weaken a form of electronic protection against target technologies connected to a person of interest. The term ‘connected’ is intended to capture technologies associated with the particular person and reflects the modern use of communications devices and services. It is narrower than the broader notion of ‘connectivity’ with the internet.

Amendment 17

Schedule 1, item 7, page 10 (before line 20)

53. This amendment inserts a definition of ‘target technology’ before the definition of ‘technical assistance notice’ in new section 317B. This amendment provides that, for purposes of new Part 15 of the Telecommunications Act:

- 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 associated with that person
- 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 associated with that person
- particular software installed, or to be installed, on a particular computer or a particular item of equipment, used, (whether directly or indirectly) or likely to be used, by a particular person is a target technology that is associated with that person
- a particular update of software that has been installed on a particular computer or a particular item of equipment that is used, (whether directly or indirectly) or likely to be used, by a particular person is a target technology that is associated with that person
- 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 associated with that person, and
- 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 associated with that person.

54. The definition also provides that, for the purpose of determining whether technology is a ‘target technology’, it is immaterial whether the person can be identified.

55. This amendment relates to amendment 16 which defines ‘systemic weakness’ and ‘systemic vulnerability’. In conjunction with amendment 16, this amendment ensures that, while systemic weaknesses or vulnerabilities cannot be built into services or devices, a

- safeguarding national security (in relation to a request given by the Director-General of Security);
- the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being (in relation to a request given by the Director-General of the ASIS);
- providing material, advice and other assistance to a person or body mentioned in subsection 7(2) of the IS Act on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means (in relation to a technical assistance request given by the Director-General of the ASD);
- enforcing the criminal law (so far as it relates to serious Australian offences) or assisting the enforcement of the criminal laws in force in a foreign country (so far as those laws relate to serious foreign offences) (in relation to a technical assistance request given by the chief officer of an interception agency).

Amendment 24 **Schedule 1, item 7, page 20 (after line 34)**

73. This amendment adds new subsection 317H(5) at the end of section 317H. Subsection 317H(5) provides that if, under subsection 317H(3), the Director-General of Security, the Director-General of ASIO, the Director-General of ASD or the chief officer of an interception agency makes a written record of a technical assistance request, the relevant Director-General or chief officer must retain the record while the request is in force. This amendment ensures that, if a technical assistance request is given orally, the written record of that request is retained for an appropriate period of time after the request is given.

Amendment 25 **Schedule 1, item 7, page 21 (after line 20)**

74. This amendment inserts new subsections (5) and (6) into new section 317HAA of the Telecommunications Act. Subsections 317HAA(1)-(4) require the Director-General of Security, the Director-General of ASIS, the Director-General of ASD or the chief officer of an interception agency to advise a designated service provider of their obligations when issued with a technical assistance request. This ensures that providers are aware that a request is voluntary.

75. This amendment provides that advice given under subsections 317HAA(1)-(4) may be given orally or in writing. If the advice is given orally, the head of the agency that has given the advice must make a written record of the advice within 48 hours after the advice was given.

Amendment 26 **Schedule 1, item 7, page 21 (before line 21)**

76. This amendment inserts new section 317HAB before new section 317HA.

77. New subsection 317HAB(1) states that 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 IGIS that the request has been given.

90. New subsection 317JA(12) states that the Director-General of ASIS must not vary a technical assistance request unless the Director-General of ASIS is satisfied that the varied request is reasonable and proportionate, and compliance with the varied request is practicable and technically feasible.

91. New subsection 317JA(13) states that the Director-General of ASD must not vary a technical assistance request unless the Director-General of ASD is satisfied that the varied request is reasonable and proportionate, and compliance with the varied request is practicable and technically feasible.

92. New subsection 317JA(14) states that the chief officer of an interception agency must not vary a technical assistance request unless the chief officer is satisfied that the varied request is reasonable and proportionate and compliance with the varied request is practicable and technically feasible.

93. New subsection 317JA(15) states that 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 IGIS that the request has been varied.

94. New subsection 317JA(16) states that if the Director-General of ASIS varies a technical assistance request, the Director-General of ASIS must, within 7 days after varying the request, notify the IGIS that the request has been varied.

95. New subsection 317JA(17) states that if the Director-General of ASD varies a technical assistance request, the Director-General of ASD must, within 7 days after varying the request, notify the IGIS that the request has been varied.

96. New subsection 317JA(18) states that 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.

97. New subsection 317JA(19) states that a failure to comply with subsection (15), (16), (17) or (18) does not affect the validity of a variation of a technical assistance request.

Amendment 29 **Schedule 1, item 7, page 24 (after line 11)**

98. This amendment inserts new subsection (1A) after new subsection 317JB(1).

99. New subsection 317JB(1A) states that 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 the request is no longer reasonable and proportionate or compliance with the request is not practicable and technically feasible, the Director-General of Security must, by written notice given to the person, revoke the request.

Amendment 30 **Schedule 1, item 7, page 24 (after line 15)**

100. This amendment inserts new subsection (2A) after new subsection 317JB(2).

101. New subsection 317JB(2A) states that if a technical assistance request has been given to a person by the Director-General of ASIS, and the Director-General of ASIS is satisfied that the request is not reasonable and proportionate or compliance with the request is not

practicable and technically feasible, the Director-General of ASIS must, by written notice given to the person, revoke the request.

Amendment 31 **Schedule 1, item 7, page 24 (after line 19)**

102. This amendment inserts new subsection (3A) after new subsection 317JB(3).

103. New subsection 317JB(3A) states that if a technical assistance request has been given to a person by the Director-General of ASD, and the Director-General of ASD is satisfied that the request is not reasonable and proportionate or compliance with the request is not practicable and technically feasible, the Director-General of ASD must, by written notice given to the person, revoke the request.

Amendment 32 **Schedule 1, item 7, page 24 (after line 22)**

104. This amendment inserts new subsections (5) – (10) after new subsection 317JB(4).

105. New subsection 317JB(5) states that 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 the request is not reasonable and proportionate or compliance with the request is not practicable and technically feasible, the chief officer must, by written notice given to the person, revoke the request.

106. New subsection 317JB(6) states that 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 IGIS that the request has been revoked.

107. New subsection 317JB(7) states that if the Director-General of ASIS revokes a technical assistance request, the Director-General of ASIS must, within 7 days after revoking the request, notify the IGIS that the request has been revoked.

108. New subsection 317JB(8) states that if the Director-General of ASD revokes a technical assistance request, the Director-General of ASD must, within 7 days after revoking the request, notify the IGIS that the request has been revoked.

109. New subsection 317JB(9) states that 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.

110. New subsection 317JB(10) states that a failure to comply with subsection (6), (7), (8) or (9) does not affect the validity of a revocation of a technical assistance request.

Amendment 33 **Schedule 1, item 7, page 24 (before line 23)**

111. This amendment inserts new section 317JC before new section 317K.

112. New section 317JC states that 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 ASIS, the Director-General of ASD or the chief officer of an interception agency, as the case requires, must have regard to the following matters:

- the interests of national security;
- the interests of law enforcement;
- the legitimate interests of the designated communications provider to whom the request relates;
- the objectives of the request;
- the availability of other means to achieve the objectives of the request;
- whether the request, when compared to other forms of industry assistance known to the Director-General of Security, the Director-General of ASIS, the Director-General of ASD 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 ASIS;
 - iii. persons whose activities are not of interest to ASD;
 - iv. persons whose activities are not of interest to interception agencies;
- whether the request is necessary;
- the legitimate expectations of the Australian community relating to privacy and cybersecurity;
- such other matters (if any) as the Director-General of Security, the Director-General of ASIS, the Director-General of ASD or the chief officer, as the case requires, considers relevant.

Amendment 34

Schedule 1, item 7, page 25 (lines 22 and 23)

113. The amendment to subparagraph 317L(2)(c)(i) removes the words “and laws imposing pecuniary penalties” and replaces them with “, so far as it relates to serious Australian offences”. The effect of the amendment is to clarify that under subparagraph 317L(2)(c)(i), for the purpose of a technical assistance notice, the specified acts or things must be by way of giving help to either ASIO or an agency, only in performance of a function, or exercise of a power, which would relate to enforcing the criminal law, only so far as it relates to a serious Australian offence.

114. This increases the threshold from a pecuniary penalty to a serious Australian offence, being 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 or for life.

Amendment 35**Schedule 1, item 7, page 25 (line 25)**

115. This amendment to subparagraph 317L(2)(c)(ii) inserts the words “so far as those laws relate to serious foreign offences”. The effect of the amendment is clarify that under subparagraph 317L(2)(c)(ii), for the purpose of a technical assistance notice, the specified acts or things must be by way of giving help to either ASIO or an agency, only in performance of a function, or exercise of a power, which would relate to enforcing the criminal law, only so far as it relates to a serious foreign offence.

Amendment 36**Schedule 1, item 7, page 25 (after line 28)**

116. This amendment inserts new subsection 317L(2A) after subsection 317L(2). Subsection 317L(2A) provides that the acts or things that a designated communications provider may be required to do in order to comply with a technical assistance notice must not be directed towards ensuring that a designated communications provider is capable of giving help to ASIO or an interception agency.

117. The effect of this amendment is to clearly differentiate between the types of acts and things a provider may be required to do under technical assistance notice, and the types of acts or things which can only be required under a technical capability notice. In contrast to subsection 317L(2A), subsection 317T(1) provides that the acts or things specified in a technical capability notice must be directed towards ensuring that the provider is capable of certain types of help to ASIO or an interception agency.

118. It clarifies that technical assistance notices are can require a provider can do things they are *already capable* of doing, as opposed to building new capabilities. To require a provider to build a new capability, a technical capability notice would be needed.

Amendment 37**Schedule 1, item 7, page 25 (line 30)**

119. This amendment omits the words ‘that may be’ from subsection 317L(3) proposed by the Bill. This amendment is consequential to amendment 38.

Amendment 38**Schedule 1, item 7, page 25 (lines 31 and 32)**

120. This amendment omits the words ‘include (but are not limited to)’ and substitutes the words ‘must be’ in subsection 317L(3) proposed by the Bill. The effect of this amendment is to make the list exhaustive and ensure that acts or things for the purposes of a technical assistance notice are all present in section 317E.

Amendment 39**Schedule 1, item 7, page 26 (after line 4)**

121. This amendment inserts new section 317LA after new section 317L.

122. New subsection 317LA(1) states that 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 the chief officer has given the AFP Commissioner a written notice setting out a proposal to give the technical assistance notice and the AFP Commissioner has approved the giving of the technical assistance notice.

132. This amendment ensures that designated communications providers who are issued with a technical assistance notice are aware of their right to make a complaint about the notice to the appropriate oversight body.

133. New subsection 317MAA(5) provides that advice under subsection (1) or (2), or notification under subsection (3) or (4), may be given orally or in writing.

134. New subsection 317MAA(6) provides that 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 make a written record of the advice or notification and do so within 48 hours after the advice or notification was given.

Amendment 42 **Schedule 1, item 7, page 27 (before line 9)**

135. This amendment inserts new section 317MAB before new section 317MA.

136. New subsection 317MAB(1) states that 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 IGIS that the notice has been given.

137. New subsection 317MAB(2) states that 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.

138. New subsection 317MAB(3) states that a failure to comply with subsection (1) or (2) does not affect the validity of a technical assistance notice.

Amendment 43 **Schedule 1, item 7, page 27 (after line 19)**

139. This amendment inserts new subsection (1A) after subsection 317MA(1). Subsection 317MA(1A) provides that an expiry date specified in a technical assistance notice must not be later than 12 months after the notice was given. This amendment ensures that a technical assistance notice cannot be in effect for longer than 12 months after the date on which it was given to the provider.

140. This prohibition applies to original notices as well as variations. The below process for extension of a notice is the vehicle for extending life of a notice beyond this 12 month limitation.

Amendment 44 **Schedule 1, item 7, page 27 (before line 20)**

141. This amendment inserts new subsections (1B), (1C), (1D), (1E), (1F) and (1G) before subsection 317MA(2).

142. New subsection 317MA(1B) provides that paragraph 317MA(1)(b) has effect subject to subsections (1C) and (1D). The effect of subsection 317MA(1B) is to provide that the general rule in paragraph 317MA(1)(b) (about when a technical assistance notice ceases to remain in force) is subject to the rules about extending a technical assistance notice in subsections 317MA(1C) and (1D).

substantial loss of evidence. However, in the vast majority of cases it is expected that the default position of consultation would apply.

Amendment 46 **Schedule 1, item 7, page 29 (line 26)**

152. This amendment omits the words ‘that may be’ from subsection 317Q(8) proposed by the Bill. This amendment is consequential to amendment 47.

Amendment 47 **Schedule 1, item 7, page 29 (line 27)**

153. This amendment omits the words ‘include (but are not limited to)’ and substitutes the words ‘must be’ in subsection 317Q(8) proposed by the Bill. The effect of this amendment is that acts or things for the purposes of a varied technical assistance notice must be acts or things that are provided in the Act as ‘listed acts or things’ in section 317E. This ensures that in relation to the variation of a technical assistance notice the list in 317E is exhaustive.

Amendment 48 **Schedule 1, item 7, page 30 (after line 11)**

154. This amendment inserts new subsection (11) – (13) after new subsection 317Q(10).

155. New subsection 317Q(11) states that a variation of a technical assistance notice must not extend the period for which the notice is in force.

156. New subsection 317Q(12) states that 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 IGIS that the notice has been varied.

157. New subsection 317Q(13) states that 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.

158. New subsection 317Q(14) states that a failure to comply with subsection (12) or (13) does not affect the validity of a variation of a technical assistance notice.

Amendment 49 **Schedule 1, item 7, page 31 (after line 4)**

159. This amendment inserts new subsections (5) – (7) after new subsection 317R(4).

160. New subsection 317R(5) states that 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 IGIS that the notice has been revoked.

161. New subsection 317R(6) states that 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.

162. New subsection 317R(7) states that a failure to comply with subsection (5) or (6) does not affect the validity of a revocation of a technical assistance notice.

Amendment 50 **Schedule 1, item 7, page 31 (line 18)**

163. This amendment inserts new paragraphs (ea) and (eb) after new paragraph 317RA(e).

164. New paragraph 317RA(ea) provides that in considering whether the requirements imposed by a technical assistance notice (including a varied notice) are reasonable and proportionate, the decision-maker must have regard to 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 as far as a person whose activities are not of interest to ASIO or the interception agency are concerned.

165. New paragraph 317RA(eb) provides that in considering whether the requirements imposed by a technical assistance notice (including a varied notice) are reasonable and proportionate, the decision-maker must have regard to whether the requirements are necessary.

166. The intention of paragraph 317RA(ea) is to provide that the potential intrusion on parties whose activities are not of interest to agencies must be considered by the decision-maker before giving a technical assistance notice.

Amendment 51 **Schedule 1, item 7, page 33 (lines 3 and 4)**

167. This amendment to subparagraph 317T(3) proposed by the Bill removes the words “and laws imposing pecuniary penalties” and replaces them with “, so far as it relates to serious Australian offences”. The effect of the amendment is to provide that, for the purpose of a technical capability notice, a relevant objective is assisting the enforcement of the criminal law as it relates to a serious Australian offence.

Amendment 52 **Schedule 1, item 7, page 33 (line 6)**

168. This amendment to subparagraph 317T(3) proposed by the Bill inserts the words “, so far as those laws relate to serious foreign offences”. The effect of the amendment is to provide that, for the purpose of a technical capability notice, a relevant objective is assisting the enforcement, in a foreign country, of a serious foreign offence.

Amendment 53 **Schedule 1, item 7, page 33 (line 23)**

169. This amendment inserts ‘Home Affairs’ before ‘Minister’ in subsection 317T(5). This amendment is consequential to amendment 7 and makes it clear that the relevant Minister is the Minister administering the TIA Act.

Amendment 54 **Schedule 1, item 7, page 33 (line 26)**

170. This amendment inserts ‘Home Affairs’ before ‘Minister’ in subsection 317T(6). This amendment is consequential to amendment 7 and makes it clear that the relevant Minister is the Minister administering the TIA Act.

Amendment 55 **Schedule 1, item 7, page 33 (line 33)**

171. This amendment inserts ‘Home Affairs’ before ‘Minister’ in paragraph 317T(6)(e). This amendment is consequential to amendment 7 and makes it clear that the relevant Minister is the Minister administering the TIA Act.

Amendment 56 **Schedule 1, item 7, page 34 (line 2)**

172. This amendment omits the words ‘that may be’ from subsection 317T(7). This amendment is consequential to amendment 57.

Amendment 57 **Schedule 1, item 7, page 34 (line 4)**

173. This amendment omits the words ‘include (but are not limited to)’ and substitutes the words ‘must be’ in subsection 317T(T). The effect of this amendment is that acts or things for the purposes of a technical capability notice must be acts or things that are provided in the Act as ‘listed acts or things’ in section 317E.

Amendment 58 **Schedule 1, item 7, page 34 (line 10)**

174. This amendment omits subsections 317T(8) to (11). This amendment is consequential to amendment 90 which replaces the content in new section 317ZGA.

Amendment 59 **Schedule 1, item 7, page 35 (after line 21)**

175. This amendment inserts new section 317TAAA after new section 317T.

176. New subsection 317TAAA(1) states that the Attorney-General must not give a technical capability notice to a designated communications provider unless the Attorney-General has given the Minister a written notice setting out a proposal to give the technical capability notice and the Minister has approved the giving of the technical capability notice.

177. New subsection 317TAAA(2) states that an approval under paragraph (1)(b) may be given orally or in writing.

178. New subsection 317TAAA(3) states that if an approval under paragraph (1)(b) is given orally, the Minister must make a written record of the approval and do so within 48 hours after the approval was given.

179. New subsection 317TAAA(4) states that the Attorney-General may make a representation to the Minister about the proposal to give the technical capability notice.

180. New subsection 317TAAA(5) states that a representation may deal with any of the matters set out in section 317ZAA and such other matters (if any) as the Attorney-General considers relevant.

181. New subsection 317TAAA(6) states that in considering whether to approve the giving of the technical capability notice, the Minister must have regard to the objectives of the notice, the legitimate interests of the designated communications provider to whom the notice relates, the impact of the notice on the efficiency and international competitiveness of the Australian telecommunications industry, the representation (if any) that was made under subsection (4) and such other matters (if any) as the Minister considers relevant.

182. The intent of this amendment is to provide for an additional layer of approval for new capabilities developed under the regime. The Minister for Communications has responsibility for the integrity and productivity of the telecommunications industry and is the relevant

portfolio minister for many of the designated communications providers listed in new section 317C. For this reason, the Minister for Communications has an important role in ensuring that requirements under a technical capability notice do not disproportionality impact a provider. The Attorney-General may make representations to the Minister for Communications regarding the underlying reasons for the notice, conditioned by the decision-making criteria that the Attorney-General must have regard to under 317ZAA. This will allow the Minister for Communications to better understand the operational reasons behind a notice, the national security and law enforcement issues that underpin the proposal and the cybersecurity and privacy impacts that the Attorney-General has taken into regard.

Amendment 60 **Schedule 1, item 7, page 35 (line 24)**

183. This amendment inserts “(1)” before the words on new section 317TAA.

Amendment 61 **Schedule 1, item 7, page 35 (after line 28)**

184. This amendment inserts (2) and (3) after new subsection 317TAA(1).

185. New subsection 317TAA(2) states that advice under subsection (1) may be given orally or in writing.

186. New subsection 317TAA(3) states that If advice under subsection (1) is given orally, the Attorney-General must make a written record of the advice and do so within 48 hours after the advice was given.

Amendment 62 **Schedule 1, item 7, page 35 (before line 29)**

187. This amendment inserts new section 317TAB before new section 317TA.

188. New subsection 317TAB(1) states that if the Attorney-General gives a technical capability notice and 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) 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 IGIS that the notice has been given.

189. New subsection 317TAB(2) states that if the Attorney-General gives a technical capability notice and 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 an interception agency in relation to a matter covered by paragraph 317T(2)(a) or 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.

190. New subsection 317TAB(3) states that a failure to comply with subsection (1) or (2) does not affect the validity of a technical capability notice.

Amendment 63**Schedule 1, item 7, page 36 (after line 7)**

191. This amendment inserts new subsection (1A) after subsection 317TA(1). Subsection 317TA(1A) provides that an expiry date specified in a technical capability notice must not be later than 12 months after the notice was given. This amendment ensures that a technical capability notice cannot be in effect for longer than 12 months after the date on which it was given to the provider.

192. This prohibition applies to original notices as well as variations. The below process for extension of a notice is the vehicle for extending life of a notice beyond this 12 month limitation.

Amendment 64**Schedule 1, item 7, page 36 (before line 8)**

193. This amendment inserts new subsections (1B), (1C), (1D), (1E) and (1F) before subsection 317TA(2).

194. New subsection 317TA(1B) states that paragraph (1)(b) has effect subject to subsection (1C).

195. New subsection 317TA(1C) states that 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.

196. New subsection 317TA(1D) states that if the Attorney-General extends the period for which a technical capability notice is in force and 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 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 IGIS of the extension.

197. New subsection 317TA(1E) states that if the Attorney-General extends the period for which a technical capability notice is in force and 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 an interception agency in relation to a matter covered by paragraph 317T(2)(a) or 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.

198. New subsection 317TA(1F) states that a failure to comply with subsection (1D) or (1E) does not affect the validity of an extension of a technical capability notice.

Amendment 65**Schedule 1, item 7, page 37 (line 13)**

199. This amendment omits “; and” and substitutes “.” in paragraph 317W(1)(b). This amendment is consequential to amendment 75.

Amendment 66**Schedule 1, item 7, page 37 (lines 14 to 16)**

200. This amendment omits paragraph 317W(1)(c). Paragraph 317W(1)(c) provided that the Attorney-General must not give a technical capability notice to a designated communications provider without first considering any copy of a report given to the Attorney-General under subsection 317W(7). Subsection 317W(7) relates to a report assessing whether or not the proposed notice would contravene section 317ZG or is reasonable, practicable or technically feasible.

201. This amendment is consequential to amendment 68, which provides that the Attorney-General must consider any report given to given under section 317WA. This amendment removes the requirement to consider the report under paragraph 317W(1)(c) to reflect the new requirement to consider and act on the recommendation of the report under new subsection 317WA(11).

Amendment 67**Schedule 1, item 7, page 38 (lines 3 to 32)**

202. This amendment omits subsections (7) - (11) and substitutes new subsections (7) - (9) after new subsection 317W(6).

203. New subsection 317W(7) states that subsection (1) does not apply to a technical capability notice proposed to be given to a designated communications provider if 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. An additional criteria is that the proposed technical capability notice comes into force immediately after the expiry of the other technical capability notice.

204. New subsection 317W(8) states that before giving a designated communications provider a technical capability notice that satisfies the following conditions 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 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.

205. New subsection 317W(9) states that 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).

Amendment 68**Schedule 1, item 7, page 38 (after line 32)**

206. This amendment inserts new section 317WA after new section 317W.

207. New section 317WA provides a framework for designated communications providers to request the carrying out of an assessment of whether a proposed technical capability notice should be given.

208. New subsection 317WA(1) provides that, 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 notice should be given.

209. New subsection 317WA(2) states that 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.

210. New subsection 317WA(3) states that for the purposes of this section, the persons appointed under subsection (2) are to be known as the assessors.

211. New subsection 317WA(4) states that one of the assessors must be a person who has knowledge that would enable the person to assess whether proposed technical capability notices would contravene section 317ZG and is cleared for security purposes to the highest level required by staff members of ASIO or such lower level as the Attorney-General approves. This should be persons with cyber security expertise or other relevant technical experts.

212. New subsection 317WA(5) states that one of the assessors must be a person who has served as a judge in one or more prescribed courts for a period of 5 years and a person who no longer holds a commission as a judge of a prescribed court. The presence of a legal expert of high standing will ensure the assessors can correctly determine the legal operation of the prohibition and scrutinise requirements in their proper legislative context.

213. New subsection 317WA(6) specifies that, as soon as practicable after appointment, the assessors must carry out an assessment of whether the notice should be given, prepare a report and give that report to the relevant parties.

214. New subsection 317WA(7) provides that, in making their assessment, the assessors must consider whether:

- the proposed technical capability notice would contravene section 317ZG (the prohibition against systemic weaknesses)
- the requirements imposed by the proposed notice are reasonable and proportionate
- compliance with the proposed notice is practicable
- compliance with the proposed notice is technically feasible, and
- it is the least intrusive measure that would be effective in achieving the legitimate objective of the proposed notice

215. In their consideration the assessors must give the most weight to whether the proposed technical capability notice would contravene section 317ZG

216. Once the assessors undertake the above assessment they must tender a report. The assessor must then give a copy of the report to the Attorney-General and the designated communications provider concerned. If the acts or things specified in the proposed technical capability notice relate to ASIO, they must give a copy of the report to the

Amendment 71**Schedule 1, item 7, page 39 (after line 28)**

225. This amendment inserts new subsections (5) – (8) after new subsection 317X(4).
226. New subsection 317X(5) states that a variation of a technical capability notice must not extend the period for which the notice is in force.
227. New subsection 317X(6) states that if the Attorney-General varies a technical capability notice in relation to ASIO, the Attorney-General must, within 7 days after varying the notice, notify the IGIS that the notice has been varied.
228. New subsection 317X(7) states that if the Attorney-General varies a technical capability notice in relation to an interception agency, the Attorney-General must, within 7 days after varying the notice, notify the Commonwealth Ombudsman that the notice has been varied.
229. New subsection 317X(8) states that a failure to comply with subsection (6) or (7) does not affect the validity of a variation of a technical capability notice.

Amendment 72**Schedule 1, item 7, page 40 (before line 1)**

230. This amendment inserts new section 317XA before new section 317Y.
231. New subsection 317XA(1) states that if a technical capability notice has been given to a designated communications provider, the Attorney-General must not vary the notice unless both the Attorney-General has given the Minister a written notice setting out a proposal to vary the technical capability notice and the Minister has approved the variation of the technical capability notice or the provider has waived compliance with subsection 317Y(2) in relation to the variation of the technical capability notice.
232. New subsection 317XA(2) states that an approval under subparagraph (1)(a)(ii) may be given orally or in writing.
233. New subsection 317XA(3) states that if an approval under subparagraph (1)(a)(ii) is given orally, the Minister must make a written record of the approval and do so within 48 hours after the approval was given.
234. New subsection 317XA(4) states that the Attorney-General may make a representation to the Minister about the proposal to vary the technical capability notice.
235. New subsection 317XA(5) states that a representation may deal with any of the matters set out in section 317ZAA and such other matters (if any) as the Attorney-General considers relevant.
236. New subsection 317XA(6) states that in considering whether to approve the variation of the technical capability notice, the Minister must have regard to the objectives of the notice as proposed to be varied, the legitimate interests of the designated communications provider to whom the notice relates, the impact of the notice as proposed to be varied on the efficiency and international competitiveness of the Australian telecommunications industry, the representation (if any) that was made under subsection (4) and such other matters (if any) as the Minister considers relevant.

237. This amendment ensures that any major variations with the potential to interact with the prohibition against systemic weaknesses are subject to the two-tiered approval process. The exception in 317XA(1)(b) allows for variation by the Attorney-General alone in circumstances where a provider has waived consultation requirements. This ensures that minor or agreed upon variations can occur without undue administrative burden and without major disrupt to government and industry activities.

Amendment 73

Schedule 1, item 7, page 40 (after line 33)

238. This amendment inserts new section 317YA after new section 317Y. Section 317YA provides a framework for assessment and reporting in relation to a technical capability notice that is varied or proposed to be varied.

239. Subsection 317YA(1) provides that if a consultation notice is given to a designated communications provider under subsection 317Y(1) in relation to a proposed variation to a technical capability notice, and 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 proposed notice would contravene section 317ZG.

240. New subsections 317YA(2) to (8) provide a framework for appointing an assessor. Subsection 317YA(3) makes clear that the person appointed to conduct the assessment is to be known as the ‘assessor’.

241. New subsection 317YA(2) states that 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.

242. New subsection 317YA(3) states that for the purposes of this section, the persons appointed under subsection (2) are to be known as the assessors.

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

244. New subsection 317YA(5) states that one of the assessors must be a person who has served as a judge in one or more prescribed courts for a period of 5 years and no longer holds a commission as a judge of a prescribed court.

245. As soon as practicable after being appointed under subsection (2), the assessors must carry out an assessment of whether the technical capability notice as proposed to be varied would contravene section 317ZG and prepare a report of the assessment.

246. New subsection 317YA(8) states that if 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 the designated communications provider concerned informs the Attorney-General that the provider no longer wants the assessment to be carried out then the

Attorney-General must direct the assessors to cease carrying out the assessment and the assessors must comply with the direction.

247. New subsection 317YA(9) states that if the assessors have begun to carry out an assessment under paragraph (6)(a) and the Attorney-General withdraws the proposed variation of the technical capability notice concerned then the Attorney-General must direct the assessors to cease carrying out the assessment and the assessors must comply with the direction.

248. The assessment process in subsection 317YA(9) and the requirement to give a copy of the report to the IGIS, in the relevant circumstances, applies both to reports into technical capability notices issued by ASIO and so-called ‘multi-agency’ reports where ASIO was merely among the parties to the technical capability notice.

249. New subsection 317YA(10) states that if a notice is given under subsection (1) in relation to a proposed variation of a technical capability notice, the Attorney-General must have regard to any report relating to the proposal to vary the technical capability notice in considering whether to proceed with the variation.

250. New subsection 317YA(11) provides that for the purposes of this Part information about the carrying out of an assessment under subsection (6) or 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.

251. New subsection 317YA(12) provides for the purposes of this section, prescribed court means the High Court or the Federal Court of Australia or the Supreme Court of a State or Territory or the District Court (or equivalent) of a State or Territory.

Amendment 74

Schedule 1, item 7, page 41 (after line 13)

252. This amendment inserts new subsections (3) – (5) after new subsection 317Z(2).

253. New subsection 317Z(3) states that if the Attorney-General revokes a technical capability notice and the acts or things specified in the revoked 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 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.

254. New subsection 317Z(4) states that if the Attorney-General revokes a technical capability notice and the acts or things specified in the revoked notice 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 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.

255. New subsection 317Z(5) states that a failure to comply with subsection (3) or (4) does not affect the validity of a revocation of a technical capability notice.

Amendment 75**Schedule 1, item 7, page 41 (after line 26)**

256. This amendment inserts new paragraph (ea) and (eb) after new paragraph 317ZAA(e).

257. New paragraph 317ZAA(ea) provides that in considering whether the requirements imposed by a technical capability notice (including a varied notice) are reasonable and proportionate, the Attorney-General must have regard to whether the requirements, when compared to other forms of industry assistance known to the Attorney-General, are the least intrusive form of industry assistance as far as a person whose activities are not of interest to ASIO or to interception agencies is concerned.

258. The intention of paragraph 317ZAA(ea) is to provide that the potential intrusion on parties whose activities are not of interest to agencies must be considered by the Attorney-General before giving a technical capability notice.

259. New paragraph 317ZAA(eb) states that in considering whether the requirements imposed by a technical capability notice (including a varied notice) are reasonable and proportionate, the Attorney-General must have regard to whether the requirements are necessary.

Amendment 76**Schedule 1, item 7, page 46 (line 9)**

260. This amendment replaces subparagraph 317ZF(1)(b)(x) with new subparagraphs (x) and (xa).

261. The effect of this amendment is to include persons appointed under new subsections 317WA(2) and 317YA(2) within the list of persons subject to the offence for unauthorised disclosure of technical assistance notice information, technical capability notice information or technical assistance request information (or information obtained in accordance with a request or notice) under subsection 317ZF(1).

262. Subsection 317WA(2) relates to the appointment of an assessor to determine the security impact, reasonableness and proportionality of a proposed technical capability notice.

Amendment 77**Schedule 1, item 7, page 47 (after line 13)**

263. This amendment inserts new subparagraphs (ixa) and (ixb) after new subparagraph 317ZF(1)(d)(ix).

264. The effect of this amendment is to include persons appointed under new subsections 317WA(2) and 317YA(2) within the category of persons who commit an offence of unauthorised disclosure if they disclose information specified in 317ZF(1)(c)(i) to 317ZF(1)(c)(iii) which has come into their knowledge or possession by virtue of their capacity as an appointee.

Amendment 78**Schedule 1, item 7, page 48 (line 3)**

265. This amendment inserts references to (5A), (5B) and (5C) in subsection 317ZF(2). The effect of this amendment is to provide that the offence of unauthorised disclosure of information in subsection 317ZF(1) does not apply if the disclosure was authorised by new

subsections 317ZF(5A), (5B) or (5C). This amendment is consequential to amendment 83, which creates a number of new exemptions to the offence in subsection 317ZF(1).

Amendment 79 **Schedule 1, item 7, page 48 (line 3)**

266. This amendment inserts references to new subsections (12A), (12B), (12C), (12D), (13), (14), (15) and (16) in subsection 317ZF(2). The effect of this amendment is to provide that the offence for unauthorised disclosure of information in subsection 317ZF(1) does not apply if the disclosure was authorised by new subsections 317ZF(12A), (12B), (12C), (12D), (13), (14), (15) or (16). This amendment is consequential to amendment 83, which creates a number of new exemptions to the offence in subsection 317ZF(1).

Amendment 80 **Schedule 1, item 7, page 48 (line 4)**

267. This amendment amends the note under 317ZF(2) to provide that new subsections (2A) and (2B), inserted by amendment 81, are to operate as exceptions to the general rule in 13.3(3) of the Criminal Code that the defendant bears an evidential burden in relation to any exception, exemption, excuse, qualification or justification provided by the law creating an offence.

Amendment 81 **Schedule 1, item 7, page 48 (after line 5)**

268. This amendment inserts new subsection (2A) and (2B) in section 317ZF.

269. New subsection 317ZF(2A) provides that, 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.

270. New subsection 317ZF(2B) provides that, 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.

271. The effect of this subsection is to provide that, if an IGIS or Ombudsman official were to be prosecuted for an offence of unauthorised disclosure of information under subsection 317ZF(1), the prosecution, not the defendant, would bear the evidential burden of providing that matters which constitute authorised disclosure under subsections (5), (5A), (5B) or (5C) of section 317ZF. This is an exception to the general rule in subsection 13.3(3) of the Criminal Code.

272. This amendment aligns the secrecy offences in the Act with secrecy offences in other laws.

Amendment 82 **Schedule 1, item 7, page 48 (line 26)**

273. This amendment inserts a new subparagraph (g) at the end of subsection 317ZF(3). Subparagraph 317ZF(3)(g) provides that a person covered by paragraph 317ZF(1)(b) may disclose technical assistance notice information, technical capability notice information or technical assistance request information to an Ombudsman official for the purpose of

exercising powers, or performing functions or duties, as an Ombudsman official. The effect of this amendment is that, if a person covered by paragraph 317ZF(1)(b) discloses a type of information specified in subsection 317ZF(3), it would not constitute an offence under subsection 317ZF(1). This ensures that information can be lawfully disclosed to Ombudsman officials.

Amendment 83

Schedule 1, item 7, page 49 (after line 4)

274. This amendment inserts new subsections (5A), (5B) and (5C) after subsection 317ZF(5). This amendment ensures that the disclosure of information by Ombudsman officials in the performance of their duties is not an offence under subsection 317ZF(1).

275. Subsection 317ZF(5A) provides that an Ombudsman official may disclose technical assistance notice information, technical capability notice information or technical assistance request information in connection with the Ombudsman official exercising powers, or performing functions or duties, as an Ombudsman official.

276. Subsection 317ZF(5B) provides that, 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.

277. Subsection 317ZF(5C) provides that, 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.

278. This amendment is designed to establish an avenue for disclosure of relevant technical assistance notice information to relevant State and Territory oversight bodies. The relevant oversight bodies are those agencies which scrutinise the interception, surveillance and law enforcement functions of state interception agencies; for instance the Inspector of the Law Enforcement Conduct Commission. It will ensure that they can have at hand the necessary information to scrutinise the activities of interception agencies under their jurisdictions.

279. The Commonwealth Ombudsman shares oversight responsibility with State and Territory oversight bodies for inspection and report of State and Territory interception activities. It is appropriate that the Ombudsman be the avenue to notify and disclosure information with its State and Territory partners.

280. ‘Technical assistance notice information’, ‘technical capability notice information’ and ‘technical assistance request information’ and ‘Ombudsman official’ are defined under section 317B.

Amendment 84

Schedule 1, item 7, page 50 (line 29)

281. This amendment inserts new subsections (12A), (12B), (12C) and (12D) after new subsection 317ZF(12).

282. New subsection 317ZF(12A) states that if the Attorney-General has given a technical capability notice and the acts or things specified in the notice are directed towards building a new capability or assisting a State or Territory interception agency, 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.

283. New subsection 317ZF(12B) states that 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 the designated communications provider or an employee of the designated communications provider or a contracted service provider of the designated communications provider or 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.

284. New subsection 317ZF(12C) states that 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 the designated communications provider or an employee of the designated communications provider or a contracted service provider of the designated communications provider or 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.

285. New subsection 317ZF(12D) states that if technical assistance notice information is disclosed under subsection (12B); or 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.

286. This amendment is designed to establish an avenue for disclosure of relevant technical capability notice information to relevant State and Territory oversight bodies. The relevant oversight bodies are those agencies which scrutinise the interception, surveillance and law enforcement functions of state interception agencies; for instance the Inspector of the Law Enforcement Conduct Commission. It will ensure that they can have at hand the necessary information to scrutinise the activities of interception agencies under their jurisdictions. Given the fact that technical capability notices may be used by multiple agencies, it is important that a central administrative body like the Communications Access Co-ordinator retain oversight of disclosures.

Amendment 85**Schedule 1, item 7, page 51 (after line 16)**

287. This amendment inserts new subsections (14), (15), (16) and (17) at the end of section 317ZF.

288. This amendment provides for the disclosure of information relating to technical assistance notices and technical capability notices by providers and their employees where the disclosure is authorised in writing by the authority who has given the notice to the provider.

289. The amendment will allow providers to disclose information about a capability to persons within their supply chain, or where otherwise relevant, with permission of the relevant Government body and subject to specified conditions. In connection with the exception to publishing statistical information in 317ZF(13), this exception will enable a provider to publically acknowledge the fact that they have received a technical capability notice and then disclose information concerning it to the necessary parties.

290. Subsections 317ZF(14)-(17) make it clear that providers and their employees may disclose information without committing an offence if:

- a technical assistance notice or technical capability notice has been given to the designated communications provider
- the designated communications provider requests that the relevant authority authorise the disclosure of the information
- the disclosure is by the provider who has been given the notice or specified employee of the provider, or a specified provider contracted to the designated service provider who has been given the notice or specified employee of the contracted provider
- the disclosure is in accordance with the conditions specified in the authorisation, and
- the disclosure is of specified information that relates to the notice.

291. Subsection 317ZF(14) provides for the disclosure of technical assistance notice information where authorised by the Director-General of Security. Subsection 317ZF(15) provides for the disclosure of technical assistance notice information where authorised by the chief officer of an interception agency. Subsection 317ZF(15) provides for the disclosure of technical capability notice information where authorised by the Attorney-General.

292. Subsection 317ZF(17) provides that an authorisation under subsection (14), (15) or (16) must be in writing.

Amendment 86**Schedule 1, item 7, page 52 (line 2)**

293. This amendment amends the heading to section 317ZG to refer to a request being made of a provider. This amendment is consequential to other amendments which extend the operation of the limitations in section 317ZG to a technical assistance request.

Amendment 87**Schedule 1, item 7, page 52 (line 5)**

294. This amendment provides that the requirement in subsection 317ZG(1) (relating to systemic weaknesses and vulnerabilities) extends to technical assistance requests. The effect of the amendment is to provide that a technical assistance request must not have the effect of:

- requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection;
- preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.

295. This amendment brings technical assistance requests into line with technical assistance notices and technical capability notices by making the prohibition against systemic weakness and systemic vulnerability uniform across the three forms of assistance.

Amendment 88 **Schedule 1, item 7, page 52 (line 7)**

296. This amendment amends the paragraph 317ZG(1)(a) to refer to a request being made of a provider. This is consequential to amendment 87 which makes the prohibition against systemic weakness and systemic vulnerability uniform across the three forms of assistance.

Amendment 89 **Schedule 1, item 7, page 52 (after line 22)**

297. This amendment inserts amendments after 317ZG(4) to clarify that, 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.

298. A similar clarification is made for systemic vulnerabilities in new subsection 4B.

299. New subsection 4C clarifies that the term ‘jeopardise the security of information’ refers to an act or thing that will, or will likely, create a material risk that otherwise secure information can be accessed by an unauthorised third party.

300. New subsection 317ZG(4A) provides that 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 317ZG(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.

301. New subsection 317ZG(4B) provides that 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.

302. New subsection 317ZG(4C) provides that 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.

4. This amendment inserts the word ‘a’ before ‘technical capability notice’ in subsection 317ZH(1).

Amendment 95 **Schedule 1, item 7, page 52 (line 28)**

5. This amendment inserts the words ‘that relates to an agency’ after ‘technical capability notice’ in subsection 317ZH(1). This amendment is intended to clarify that the prohibition in 317ZH(1) extends to warrants and authorisations that the particular relevant agency would require.

Amendment 95 **Schedule 1, item 7, page 52 (line 30)**

6. This amendment inserts the words ‘the agency, or an officer of the agency, would be required to have or obtain’ before ‘a warrant or authorisation under any of the following laws’ in subsection 317ZH(1). This amendment makes clear that a technical assistance notice or a technical capability notice is not intended to require a provider to do an act or thing that, if the act or thing was to be done by an agency or an officer of an agency, would require a warrant or authorisation under a law provided in paragraphs 317ZH(a) to (g).

Amendment 96 **Schedule 1, item 7, page 52 (line 31)**

7. This amendment omits the words ‘is required’ from subsection 317ZH(1). This amendment is consequential to amendment 95.

Amendment 97 **Schedule 1, item 7, page 53 (line 3)**

8. This amendment omits paragraph 317ZH(1)(e). The effect of this amendment is to provide that a technical assistance notice or technical capability notice has effect despite requiring a designated communications provider to do an act or thing for which a warrant or authorisation would be required under the IS Act.

9. The IS Act contains ministerial authorisations for ASIS and ASD. As ASIS and ASD cannot issue a technical assistance notice or request the issue of a technical capability notice (the powers subject to the prohibition in section 317ZH). Explicitly mentioning the IS Act does not provide a meaningful safeguard.

10. The removal of this provision is not intended to expand the potential requirements of a notice issued by these agencies. The amendment is intended to resolve the ambiguities that arise from explicitly including the IS Act and the ministerial authorisations within that Act that do not apply to the agencies limited by 317ZH.

Amendment 98 **Schedule 1, item 7, page 53 (line 5)**

11. This amendment omits the reference to paragraph (e) in paragraph 317ZH(1)(f). This amendment is consequential to amendment 97 which omits paragraph 317ZH(1)(e).

Amendment 99 **Schedule 1, item 7, page 54 (after line 16)**

12. This amendment inserts new subsections (6) to (9) at the end of section 317ZH. Subsections 317ZH(6) to (9) define a number of concepts for the purposes of section 317ZH.

13. Subsection 317ZH(6) defines when a technical assistance notice relates to an agency for the purposes of section 317ZH. Subsection 317ZH(6) provides that a notice relates to ASIO if the notice was given by the Director-General of Security, and a notice relates to an interception agency if the notice was given by the chief officer of that interception agency.
14. Subsection 317ZH(7) defines when a technical capability notice relates to an agency for the purposes of section 317ZH.
15. Subsection 317ZH(7) provides that a notice relates to ASIO if the acts or things specified in the notice are either 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 are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b).
16. Similarly, subsection 317ZH(7) provides that a technical capability notice relates to an interception agency if the acts or things specified in the notice are either 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 are by way of giving help to the interception agency in relation to a matter covered by paragraph 317T(2)(b).
17. The concept of ‘capable of giving help’ goes to the new capability aspects of technical capability notices. Requirements on a provider to be ‘capable of giving help’ are requirements to build a new capability which can then be used. The concept of ‘giving help’ is conduct that a provider is already capable of giving, whether through their existing functions or by virtue of a new capability constructed under a technical capability notice.
18. These amendments to 317ZH are intended to clarify the prohibition on technical assistance notices and technical capability notices being used as a substitute for warrants or authorisations. They have the effect of clarifying that the prohibition applies if the relevant issuing agency would otherwise need a warrant or authorisation to undertake the conduct required by the notice. This ensures that agencies under 317ZH are limited by the warrants or authorisations that they themselves would require, rather than a warrant or authorisation that another authority would require to lawfully do the things within the notice.
19. Subsection 317ZH(8) provides a definition of ‘agency’ for the purposes of section 317ZH. Agency is defined as either ASIO or an interception agency.
20. Subsection 317ZH(9) provides that, for the purposes of section 317ZH, ‘officer of an agency’ means the Director-General of Security or an ASIO employee in relation to ASIO, and the chief officer or an officer of the interception agency in relation to an interception agency.

Amendment 100

Schedule 1, item 7, page 55 (line 17)

21. This amendment inserts the words ‘declares in writing that the Director-General of Security’ after ‘Director-General of Security’ in paragraph 317ZK(1)(c). This amendment provides that subsection 317ZK(1) will not apply if, 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 he or she is satisfied that it would be contrary to the public

interest for this section to apply to the requirement. The effect of this amendment is to require that a decision that subsection 317ZK(1) should not apply must be by declaration in writing.

Amendment 101 **Schedule 1, item 7, page 55 (line 22)**

22. This amendment inserts the words ‘declares in writing that the chief officer’ after ‘chief officer’ in paragraph 317ZK(1)(d). This amendment provides that subsection 317ZK(1) will not apply if, 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 he or she is satisfied that it would be contrary to the public interest for this section to apply to the requirement. The effect of this amendment is to require that a decision that subsection 317ZK(1) should not apply must be by declaration in writing.

Amendment 102 **Schedule 1, item 7, page 55 (line 25)**

23. This amendment inserts the words ‘declares in writing that the Attorney-General’ after ‘Attorney-General’ in paragraph 317ZK(1)(e). This amendment provides that subsection 317ZK(1) will not apply if, in the case of a requirement under a technical capability notice given by the Attorney-General, the Attorney-General declares in writing that he or she is satisfied that it would be contrary to the public interest for this section to apply to the requirement. The effect of this amendment is to require that a decision that subsection 317ZK(1) should not apply must be by declaration in writing.

Amendment 103 **Schedule 1, item 7, page 55 (line 32)**

24. This amendment relates to the decision about whether it would be contrary to the public interest for section 317ZK (about terms and conditions on which help is to be given etc.) to apply. The amendment clarifies that, 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 chief officer must have regard to the interests of law enforcement.

Amendment 104 **Schedule 1, item 7, page 55 (line 33)**

25. This amendment relates to the decision about whether it would be contrary to the public interest for section 317ZK (about terms and conditions on which help is to be given etc.) to apply. The amendment clarifies that, 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 Director-General must have regard to the interests of national security.

Amendment 105 **Schedule 1, item 7, page 56 (lines 14 and 15)**

26. This amendment inserts new paragraphs (c) to (f) in subsection 317ZK(3). This amendment provides that the designated communications provider must comply a requirement under a technical assistance notice or a technical capability notice on the basis that the provider neither profits from complying nor bears the reasonable costs of complying, unless:

- the provider and the applicable costs negotiator otherwise agree

- 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
- 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
- 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.

27. These amendments allow decision-makers to selectively apply the public interest exemption to particular parts of 317ZK. This effectively allows decision-makers to ‘turn off’ some conditions in section 317ZK and apply others, providing for greater flexibility in the exercise of the public interest exemption. By way of example, it may be appropriate in some cases to allow for terms and conditions to be set in accordance with 317ZK but not full cost recovery.

Amendment 106 **Schedule 1, item 7, page 56 (after line 16)**

28. This amendment inserts new subsection (3A) after subsection 317ZK(3). Subsection 317ZK(3A) sets out the matters which must be considered by the Director-General of Security, the chief officer or the Attorney-General in deciding whether the subsection 317ZK(3) presumption (as to who should bear the cost of assistance) should apply. The authority who has given the notice must have regard to the interests of law enforcement (in the case of an interception agency), the interests of national security (in the case of ASIO), the objects of this Act, the extent to which compliance with the requirement will impose a regulatory burden on the provider, the reasons for the giving of the technical assistance notice or technical capability notice, as the case requires, as well as 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.

29. The existing measures in 317ZK set a high threshold for exercising the public interest exemption in subsection 317ZK(3) by requiring that the decision-maker take into account a range of commercial, law-enforcement and security considerations.

Amendment 107 **Schedule 1, item 7, page 57 (after line 2)**

30. This amendment inserts new subsection (6A) and (6B) after subsection 317ZK(6).

31. Subsection 317ZK(6A) creates a public interest exemption to the requirement in subsection 317ZK(4) that the provider must comply with the requirement on such terms as agreed between the provider and the applicable costs negotiator, or as determined by an arbitrator. The effect of subsection 317ZK(6A) is to allow the authority who has given the technical assistance notice or technical capability notice to declare in writing that he or she is satisfied that it would be contrary to the public interest for subsection 317ZK(4) to apply to a requirement in the notice.

32. Subsection 317ZK(6B) sets out the matters which must be considered by the Director-General of Security, the chief officer or the Attorney-General in deciding whether the subsection 317ZK(4) should apply. The authority who has given the notice must have regard to the interests of law enforcement (in the case of an interception agency), the interests of national security (in the case of ASIO), the objects of this Act, the extent to which compliance with the requirement will impose a regulatory burden on the provider, the reasons for the giving of the technical assistance notice or technical capability notice, as the case requires, as well as 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. The effect of this amendment is to set a high threshold for exercising the public interest exemption under subsection 317ZK(6A) by requiring that the decision-maker take into account a range of commercial, law-enforcement and security considerations.

33. These amendments allow decision-makers to selectively apply the public interest exemption to particular parts of 317ZK. This effectively allows decision-makers to ‘turn off’ some conditions in section 317ZK and apply others, providing for greater flexibility in the exercise of the public interest exemption.

Amendment 108 **Schedule 1, item 7, page 57 (line 8)**

34. This amendment inserts the words ‘Home Affairs’ before the word ‘Minister’ in subsection 317ZK(8). This amendment is consequential to amendment 7 and makes it clear that the relevant Minister is the Minister administering the TIA Act.

Amendment 109 **Schedule 1, item 7, page 57 (line 14)**

35. This amendment inserts the words ‘Home Affairs’ before the word ‘Minister’ in subsection 317ZK(11). This amendment is consequential to amendment 7 and makes it clear that the relevant Minister is the Minister administering the TIA Act.

Amendment 110 **Schedule 1, item 7, page 57 (line 17)**

36. This amendment inserts the words ‘Home Affairs’ before the word ‘Minister’ in subsection 317ZK(12). This amendment is consequential to amendment 7 and makes it clear that the relevant Minister is the Minister administering the TIA Act.

Amendment 111 **Schedule 1, item 7, page 57 (line 21)**

37. This amendment inserts the words ‘Home Affairs’ before the word ‘Minister’ in subsection 317ZK(14). This amendment is consequential to amendment 7 and makes it clear that the relevant Minister is the Minister administering the TIA Act.

Amendment 112 **Schedule 1, item 7, page 58 (after line 10)**

38. This amendment adds new subsections (17) to (20) at the end of section 317ZK.

39. Subsection 317ZK(17) provides that for the purposes of section 317ZK a technical capability notice relates to ASIO if 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
- are by way of giving help to ASIO in relation to a matter covered by paragraph 317T(2)(b).

40. For the purposes of new subsection 317ZK(17), notices that ‘relate to ASIO’ include so-called ‘multi-agency’ technical capability notices issued for the purposes of assisting ASIO.

41. Subsection 317ZK(18) provides that for the purposes of section 317ZK a technical capability notice relates to an interception agency if 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 the interception agency in relation to a matter covered by paragraph 317T(2)(a); or
- are by way of giving help to the interception agency in relation to a matter covered by paragraph 317T(2)(b).

42. The issue of whether a notice relates to ASIO or to an interception agency is relevant to subsection 317ZK(2) under which the Director-General or the chief officer, as the case may be, must have regard to the interests of national security and law enforcement, respectively, in deciding whether it would be contrary to the public interest for section 317ZK to apply.

43. Subsection 317ZK(19) provides that, for the purposes of Part 15 of the Telecommunications Act, information about a declaration under paragraph 317ZK(1)(c), (1)(d), (3)(d), (3)(e), (6A)(a) or (6A)(b) is taken to be information about a technical assistance notice.

44. Subsection 317ZK(20) provides that, for the purposes of Part 15 of the Telecommunications Act, information about a declaration under paragraph 317ZK(1)(e), (3)(f) or (6A)(c) is taken to be information about a technical capability notice.

45. The effect of subsections 317ZK(19) and (20) is to ensure that information about a declaration under the relevant paragraphs of section 317ZK is included within the definitions of technical capability notice information and technical assistance notice information under section 317B and is, consequently, protected by the information disclosure provisions in sections 317ZF and 317ZFA.

Amendment 113**Schedule 1, item 7, page 58 (before line 11)**

46. This amendment inserts new section 317ZKA before section 317ZL.

47. These amendments ensure that when decision-makers deviate from the default no-profit/no-loss basis for industry assistance oversight bodies are notified. This deviation may only be undertaken for strict public interest reasons in exceptionally rare cases, such as where a provider's actions have recklessly created a security risk or wilfully facilitated criminal activities and it would be improper to fully compensate them for assistance given.

48. Subsections 317ZKA(1), (2) and (3) ensure that the relevant oversight body is notified when an authority who has given a technical assistance notice or technical capability notice declares that it would be contrary to the public interest for section 317ZK, subsection 317ZK(3) or 317ZK(4) to apply to a requirement in the notice.

49. Subsection 317ZKA(1) provides that, 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 IGIS of the making of the declaration.

50. Subsection 317ZKA(2) provides that, 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.

51. Subsection 317ZKA(3) provides that, if the Attorney-General makes a declaration under paragraph 317ZK(1)(e), (3)(f) or (6A)(c) in relation to a technical capability notice and the acts or things specified in the notice are either 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 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 IGIS of the making of the declaration.

52. Subsection 317ZKA(4) provides that, if the Attorney-General makes a declaration under paragraph 317ZK(1)(e), (3)(f) or (6A)(c) in relation to a technical capability notice and the acts or things specified in the notice are either 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 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.

53. Subsection 317ZKA(5) provides that a failure to comply with subsection (1), (2), (3) or (4) does not affect the validity of a declaration under paragraph 317ZK(1)(c), (1)(d), (1)(e), (3)(d), (3)(e), (3)(f), (6A)(a), (6A)(b) or (6A)(c).

Amendment 114**Schedule 1, item 7, pages 60 and 61 (table item 2)**

54. This amendment omits table item 2 from new section 317ZM.

55. This amendment removes the Australian Commission for Law Enforcement Integrity from the definition of ‘interception agency’.

Amendment 115 **Schedule 1, item 7, page 61 (table item 3)**

56. This amendment omits table item 3 from new section 317ZM.

57. This amendment removes the Australian Crime Commission from the definition of ‘interception agency’.

Amendment 116 **Schedule 1, item 7, page 61 (table item 5)**

58. This amendment omits table item 5 from new section 317ZM.

59. This amendment removes the Independent Commission Against Corruption of New South Wales from the definition of ‘interception agency’.

Amendment 117 **Schedule 1, item 7, pages 61 and 62 (table item 6)**

60. This amendment omits table item 6 from new section 317ZM.

61. This amendment removes the New South Wales Crime Commission from the definition of ‘interception agency’.

Amendment 118 **Schedule 1, item 7, page 62 (table item 7)**

62. This amendment omits table item 7 from new section 317ZM.

63. This amendment removes the Law Enforcement Conduct Commission of New South Wales from the definition of ‘interception agency’.

Amendment 119 **Schedule 1, item 7, page 62 (table item 8)**

64. This amendment omits table item 8 from new section 317ZM.

65. This amendment removes the Independent Broad-based Anti-corruption Commission of Victoria from the definition of ‘interception agency’.

Amendment 120 **Schedule 1, item 7, pages 62 and 63 (table item 9)**

66. This amendment omits table item 9 from new section 317ZM.

67. This amendment removes the Crime and Corruption Commission of Queensland from the definition of ‘interception agency’.

Amendment 121 **Schedule 1, item 7, page 63 (table item 10)**

68. This amendment omits table item 10 from new section 317ZM.

69. This amendment removes the Independent Commissioner Against Corruption (SA) from the definition of ‘interception agency’.

Amendment 122 **Schedule 1, item 7, page 63 (table item 11)**

70. This amendment omits table item 11 from new section 317ZM.
71. This amendment removes the Corruption and Crime Commission (WA) from the definition of ‘interception agency’.

Amendment 123 **Schedule 1, item 7, page 65 (table item 2)**

72. This amendment omits table item 2 from new section 317ZR.
73. This amendment removes the Australian Commission for Law Enforcement Integrity from the table that lists the potential delegates of an ‘interception agency’.

Amendment 124 **Schedule 1, item 7, page 65 (table item 3)**

74. This amendment omits table item 3 from new section 317ZR.
75. This amendment removes the Australian Crime Commission from the table that lists the potential delegates of an ‘interception agency’.

Amendment 125 **Schedule 1, item 7, page 65 (table item 5)**

76. This amendment omits table item 5 from new section 317ZR.
77. This amendment removes the Independent Commission Against Corruption of New South Wales from the table that lists the potential delegates of an ‘interception agency’.

Amendment 126 **Schedule 1, item 7, page 65 (table item 6)**

78. This amendment omits table item 6 from new section 317ZR.
79. This amendment removes the New South Wales Crime Commission from the table that lists the potential delegates of an ‘interception agency’.

Amendment 127 **Schedule 1, item 7, page 65 and 66 (table item 7)**

80. This amendment omits table item 7 from new section 317ZR.
81. This amendment removes the Law Enforcement Conduct Commission of New South Wales from the table that lists the potential delegates of an ‘interception agency’.

Amendment 128 **Schedule 1, item 7, page 66 (table item 8)**

82. This amendment omits table item 8 from new section 317ZR.
83. This amendment removes the Independent Broad-based Anti-corruption Commission of Victoria from the table that lists the potential delegates of an ‘interception agency’.

Amendment 129 **Schedule 1, item 7, page 66 (table item 9)**

84. This amendment omits table item 9 from new section 317ZR.

85. This amendment removes the Crime and Corruption Commission of Queensland from the table that lists the potential delegates of an ‘interception agency’.

Amendment 130 **Schedule 1, item 7, page 66 (table item 10)**

86. This amendment omits table item 10 from new section 317ZR.

87. This amendment removes the Independent Commissioner Against Corruption (SA) from the table that lists the potential delegates of an ‘interception agency’.

Amendment 131 **Schedule 1, item 7, page 67 (after line 7)**

88. This amendment inserts new section 317ZRA in the Telecommunications Act. Section 317RA clarifies the relationship of new Part 15 of the Telecommunications Act to parliamentary privileges and immunities. It provides that Part 15 does not affect the law relating to the powers, privileges and immunities of either House of the Parliament or the members, committees or joint committees of either House of Parliament.

Amendment 132 **Schedule 1, item 7, page 67 (before line 8)**

89. This amendment inserts new section 317ZRB after new section 317ZS. New section 317ZRB establishes an express inspection power of Part 15 for the Commonwealth Ombudsman. The intent of this amendment is to make clear that the Ombudsman may inspect the records of an interception agency to determine compliance with this Part independent of the Ombudsman’s inherent powers within the Ombudsman Act 1976

90. New subsection 317ZRB(1) states that an Ombudsman official may inspect the records of an interception agency to determine the extent of compliance with this Part by the agency and the chief officer of the agency and officers of the agency.

91. New subsection 317ZRB(2) states that 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).

92. New subsection 317ZRB(3) states that the Commonwealth Ombudsman may make a written report to the Home Affairs Minister on the results of one or more inspections under subsection (1).

93. New subsection 317ZRB(4) states that a report under subsection (3) must not include information which, if made public, could reasonably be expected to prejudice an investigation or prosecution or compromise any interception agency’s operational activities or methodologies.

94. New subsection 317ZRB(5) states that if the Commonwealth Ombudsman makes a report under subsection (3) and the report relates to an inspection under subsection (1) of the records of an interception agency of a State or Territory then the Commonwealth Ombudsman must give a copy of the report to the chief officer of the interception agency.

95. New subsection 317ZRB(6) states that 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.

96. New subsection 317ZRB(7) states that 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 prejudice an investigation or prosecution or compromise any interception agency's operational activities or methodologies.

97. This inspection function is not mandatory but allows the Ombudsman to effectively act on notifications or complaints the organisation may receive through agency exercise of industry assistance measures. It complements the express powers to inspect records on the exercise of Part 15 powers including in the existing inspection regimes of the TIA Act and SD Act.

Amendment 133 **Schedule 1, item 7, page 67 (line 9)**

98. This amendment inserts the words 'Home Affairs' before the word 'Minister' in subsection 317ZS(1). This makes it clear that the relevant Minister is the Minister administering the TIA Act.

Amendment 134 **Schedule 1, item 7, page 67 (line 21)**

99. This amendment inserts new paragraph 317ZS(1)(d) to provide that, in addition to the requirements in paragraphs 317ZS(1)(a) to (c) relating to annual reports, the annual reports prepared under section 317ZS must include information on the kinds of serious Australian offences for which Schedule 1 powers are used in relation to. This will be similar to reporting on offences already contained within this annual report. For example, the annual report notes the offence types for which interception warrants or data authorisations were issued and authorised.

Amendment 135 **Schedule 1, page 67 (after line 32) after item 7**

100. This amendment inserts items 7A and 7B at the end of Part 1 of Schedule 1. This amendment provides for maximum penalties for body corporates and persons other than body corporates for contraventions of the civil penalty provisions in subsections 317ZA(1) and (2) for failing to comply with a requirement under a technical assistance notice or a technical capability notice.

101. New paragraph 570(3)(aa) in the Telecommunications Act provides that, in the case of a contravention the civil penalty provisions in subsection 317ZA(1) or (2), the pecuniary penalty payable by a body corporate is not to exceed 47,619 penalty units for each contravention.

102. New paragraph (4D) provides that 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.

103. New paragraph (4C) provides that subsection 570(4), which establishes a maximum penalty payable under subsection (1) by a person other than a body corporate, does not apply to a contravention of subsection 317ZA(1) or (2). The effect of paragraph (4C) is to provide

that the maximum penalty for each contravention of subsections 317ZA(1) or (2) by a person other than a body corporate may exceed \$50,000.

Amendment 136 **Schedule 1, page 68 (before line 1), before the heading**

104. This amendment inserts item 7C which adds subsection 83(4) to allow for inspections of records of technical assistance requests, technical assistance notices and technical capability notices under Part 15 of the Telecommunications Act when the measures have been used in connection with an interception warrant.

105. Assistance from the communications industry is critical to the effective exercise of TIA Act powers, including interception warrants. In many cases, requests or requirements to industry will be made to ensure that these powers can be used to obtain the authorised evidence or intelligence.

106. As the new industry assistance measures compliment these existing TIA Acts powers, new subsection 83(4) will ensure that the Commonwealth Ombudsman can oversight their joint use.

Amendment 137 **Schedule 1, page 68, after proposed item 7C**

107. This amendment inserts item 7D which adds subsection 84(1) to ensure that period Ombudsman reports on interception warrants include any inspection activities related to the new industry assistance measures in Part 15 of the Telecommunications Act.

Amendment 138 **Schedule 1, page 68, after proposed item 7D**

108. This amendment inserts item 7E which adds subsection 186B(1A) of the TIA Act to allow for inspections of technical assistance requests, technical assistance notices and technical capability notices under Part 15 of the Telecommunications Act when the measures have been used in conjunction with a stored communications warrant or data authorisation.

109. Assistance from the communications industry is critical to the effective exercise of TIA Act powers, including stored communications warrants and data authorisations. In many cases, requests or requirements to industry will be made to ensure that these powers can be used to obtain the authorised evidence or intelligence.

110. As the new industry assistance measures compliment these existing TIA Acts powers new subsection 186B(1A) will ensure that the Commonwealth Ombudsman can oversight their joint use.

Amendment 139 **Schedule 1, page 68, after proposed item 7E**

111. This amendment amends item 7F which includes new section 187N of the TIA Act. This amendment provides for a review of the operation of the amendments made by the Bill by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). By amending 187N, this amendment provides that the review of the amendment made by this Bill must be reviewed by the Committee within the same timeframes the compulsory review of Part 5-1A of the TIA Act.

112. This is an important public accountability and transparency measure. It will provide for a review of the amendments made by the Bill three years after the conclusion of the ‘implementation phase’ as defined in subsection 187N(2) of the TIA Act. ‘Implementation phase’ is defined in subsection 187H(2) as the period of 18 months starting on the commencement of Part 5-1A. As Part 5-1A commenced on 13 October 2015, the PJCIS must commence its review of both the operation of Part 5-1A and the amendments made by the Bill on 13 April 2019. It must conclude its review by 13 April 2020.

113. This amendment inserts item 7G which adds new subsection 187N(1). This inserts “and the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018” after “this Part” in subsection 187N(1) TIA Act.

Amendment 140 **Schedule 2, page 70 (after line 8)**

114. This amendment inserts new subsection 25A(4A) of the ASIO Act to provide for the return of a computer or other thing under a computer access warrant. Subsection 25A(4A) provides that where a warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph 25A(4)(ac), and the computer or other thing is so removed from the premises, then the computer or thing must be returned to the premises. If returning the computer or thing would be prejudicial to security, then returning the computer or other thing should occur when the return would no longer be prejudicial to security. Otherwise, the return should occur within a reasonable period.

Amendment 141 **Schedule 2, item 7, page 71 (after line 11)**

115. This amendment inserts new subsections (9) and (10) after new subsection 25A(8) of the ASIO Act to provide for the return of and dealing with a computer or other thing under a computer access warrant.

116. Subsection 25A(9) states that subsection (8) does not authorise the doing of a thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or 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). Further, subsection 8 does not authorise the doing of a thing that is like to cause any other material loss or damage to other persons lawfully using a computer.

117. New subsection 25A(10) states that where a computer or other thing is removed from a place in accordance with paragraph 25A(8)(f), the computer or thing must be returned to that place. If returning the computer or thing would be prejudicial to security, then returning the computer or other thing should occur when the return would no longer be prejudicial to security. Otherwise, the return should occur within a reasonable period.

Amendment 142 **Schedule 2, item 8, page 72 (after line 14)**

118. This amendment inserts new subsection (3D) and (3E) after subsection 27A(3C) of the ASIO Act to provide for the return of a computer or other thing under a computer access warrant. New subsection 27A(3D) provides that subsection (3C) does not authorise the doing of a thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or 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). Subsection (3C)

further does not authorise the doing of a thing that is likely to cause any other material loss or damage to other persons lawfully using a computer.

119. New subsection 27A(3E) provides that where a computer or other thing is removed from a place in accordance with paragraph 27A(3C)(f), the computer or thing must be returned to that place. If returning the computer or thing would be prejudicial to security, then returning the computer or other thing should occur when the return would no longer be prejudicial to security. Otherwise, the return should occur within a reasonable period.

Amendment 143 **Schedule 2, page 72 (after line 34)**

120. This amendment inserts new subsection 27E(3A) of the ASIO Act to provide for the return of a computer or other thing under a computer access warrant. Subsection 27E(3A) provides that where a warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph 27E(2)(da), and the computer or other thing is so removed from the premises, then the computer or thing must be returned to the premises. If returning the computer or thing would be prejudicial to security, then returning the computer or other thing should occur when the return would no longer be prejudicial to security. Otherwise, the return should occur within a reasonable period.

Amendment 144 **Schedule 2, item 12, page 74 (after line 2)**

121. This amendment inserts new subsections (7) and (8) after subsection 27E(6) of the ASIO Act to provide for the return of a computer or other thing under a computer access warrant.

122. New subsection 27E(7) states that Subsection (6) does not authorise the doing of a thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or 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). Subsection (6) further does not authorise the doing of a thing that is likely to cause any other material loss or damage to other persons lawfully using a computer.

123. New subsection 27E(8) provides that where a computer or other thing is removed from a place in accordance with paragraph 27E(6)(f), the computer or thing must be returned to that place. If returning the computer or thing would be prejudicial to security, then returning the computer or other thing should occur when the return would no longer be prejudicial to security. Otherwise, the return should occur within a reasonable period.

Amendment 145 **Schedule 2, page 74 (after line 4), after item 13**

124. This is a consequential amendment to section 34.

Amendment 146 **Schedule 2, page 74 (after line 19), after item 16**

125. This amendment inserts item 16A which adds new section 34A after section 34 in the ASIO Act. New section 34A provides for the Director-General of Security to report on concealment of access activities to the Attorney-General.

126. New subsection 34A(1) states that if a warrant issued under this Division has ceased to be in force and 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 the thing has not been dealt with in a report under subsection 34(1) the Director-General must 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 do so as soon as practicable after the end of that period.

127. New subsection 34A(2) states that if a warrant issued under this Division has ceased to be in force and 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 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 do so as soon as practicable after the end of that period.

128. New subsection 34A(3) states that For the purposes of this section, each of the following periods is a prescribed post-cessation period of a warrant the 3-month period beginning immediately after the warrant ceased to be in force each subsequent 3-month period.

Amendment 147 **Schedule 2, item 49, page 89 (line 35)**

129. This amendment adds subparagraph (xii) to paragraph 27D(1)(b). The amendment provides that a computer access warrant specify any conditions to which things may be done under the warrant. The effect of the amendment is that, where an eligible judge or nominated AAT issues a computer access warrant, the warrant must specify any conditions under which things must be done under the warrant.

Amendment 148 **Schedule 2, item 49, page 92 (after line 8)**

130. This amendment inserts new subsection 27E(2A) of the SD Act to provide for the return of a computer or other thing under a computer access warrant. Subsection 27E(2A) provides that where a warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph 27E(2)(f), and the computer or other thing is so removed from the premises, then the computer or thing must be returned to the premises within a reasonable period.

Amendment 149 **Schedule 2, item 49, page 94 (after line 16)**

131. This amendment inserts new subsections (8) and (9) after subsection 27E(7) of the SD Act to provide for the return of a computer or other thing under a computer access warrant.

132. New subsection 27E(8) states that subsection (7) does not authorise the doing of a thing that is likely to materially interfere with, interrupt or obstruct a communication in transit or 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). Further subsection (7) does not authorise the doing of a thing that is likely to cause any other material loss or damage to other persons lawfully using a computer.

133. Subsection 27E(9) provides that where a computer or other thing is removed from a place in accordance with paragraph 27E(7)(f), the computer or thing must be returned to the place within a reasonable period.

Amendment 150**Schedule 2, item 49, page 99 (after line 23)**

134. This amendment inserts new section 27J of the SD Act to clarify the relationship between Division 4 (Computer access warrants) of Part 2 of the SD Act and parliamentary privileges and immunities. Section 27J provides that to avoid doubt Division 4 does not affect the law relating to the powers, privileges and immunities of any of the following:

- each House of the Parliament;
- the members of each House of the Parliament;
- the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

135. The purpose of the amendment is to clarify that the provisions relating to computer access warrants in Division 4 of Part 2 of the SD Act are not intended to intrude on the powers, privileges and immunities of the Parliament.

Amendment 151**Schedule 2, page 102 (after line 26), after item 60**

136. This amendment inserts item 60A. Item 60A amends subsection 32(4) of the SD Act to provide that the subsection 32(2A) (proposed by clause 60 of this Bill) is not captured by subsection 32(4) of the SD Act, which provides that nothing in Part 3 of that Act (relating to emergency authorisations) authorises the doing of anything for which a warrant would be required under the TIA Act. The effect of this amendment is to give proper effect to subsection 32(2A) such that an emergency authorisation for access to data held in a computer may authorise anything that a computer access warrant may authorise.

Amendment 152**Schedule 2, page 118 (after line 28), after item 104**

137. This amendment inserts new section 49B in the SD Act. This amendment ensures that the Commonwealth Ombudsman is notified when an act or thing is done to conceal access under a computer access warrant more than 28 days after the warrant has expired.

138. This amendment relates to acts or things done under new subsection 27E(7). New subsection 27E(7) of the SD Act provides that a computer access warrant will also authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to a computer under a computer access warrant. Paragraph 27E(7)(k) allows concealment activities to be done at any time while the warrant is in force, or within 28 days after it ceases to be in force, or at the earliest time after this period at which it is reasonably practicable to do so.

139. New section 49B provides that, if a computer access warrant was issued in response to an application made by a law enforcement officer of a law enforcement agency, and one or more things mentioned in subsection 27E(7) were done under the warrant after the 28-day period following expiry of the warrant, the chief officer of the law enforcement agency must notify the Ombudsman as soon as practicable after the concealment activity was done.

Amendment 153**Schedule 2, page 121 (after line 29), after item 111**

140. This amendment amends section 55 of the SD Act to include new measures within Part 15 of the Telecommunications Act within the Commonwealth Ombudsman's existing inspection regime. The item bridges an oversight gap that may have been present in cases where industry assistance measures are used in connection with surveillance device warrants.

141. Item 111A provides that the Ombudsman may inspect records relating to the performance of Part 15 powers that have been used in connection with a surveillance device warrant, including computer access warrants. Part 15 powers include technical assistance requests, technical assistance notices and technical capability notices introduced by Schedule 1 of this Bill.

142. Their inclusion in the existing inspection regime in the SD Act reflects the fact that these industry assistance measures will be used in connection with underlying surveillance device warrants. Communications providers are in a unique position to undertake activities to ensure surveillance device powers under warrant can be utilised effectively.

Amendment 154 Schedule 2, page 122 (after line 9), after item 113

143. This amendment inserts items 113A and 113B.

144. Item 113A amends section 64 of the SD Act to move the existing content in section 64 into a subsection. This amendment is consequential item 113B.

145. Item 113B inserts subsection (2) into section 64 of the SD Act to provide for circumstances in which the Commonwealth is liable to pay a person who has suffered loss or injury flowing from a computer access warrant. Section 64 provides that the Commonwealth is liable to pay a person who has suffered loss or injury resulting from:

- the use of one or more of the following for the purpose of obtaining access to data that is held in the computer:
 - a computer; or
 - a telecommunications facility operated or provided by the Commonwealth or a carrier; or
 - any other electronic equipment; or
 - a data storage device
- where the use of the computer, facility, equipment or device, as the case may be, was by any of the following:
 - the Australian Federal Police
 - the Integrity Commissioner or staff member of the Australian Commission for Law Enforcement Integrity; or
 - the Australian Crime Commission
- and 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
 - is neither in accordance with the SD Act or in the performance of a function, of the exercise of a power, conferred by a law of the Commonwealth.

146. Paragraphs 64(2)(e) and (f) provide that the amount to be paid to the person is the amount of compensation that is agreed between the person and the Commonwealth or, in default of such an agreement, the amount of compensation that is determined in a court.

147. The intention of subsection 64(2) is to provide a person an avenue for obtaining compensation from the Commonwealth in situations where a Commonwealth officer within the above organisations undertakes, without proper authority, activities consistent with what would otherwise be permissible by a lawful computer access warrant. The core activity authorised under a warrant is the fact of access to a computer through the telecommunications network or other computer equipment and the provision encompasses these actions. Persons who suffer loss or injury as a result of computer access that is inconsistent with the Commonwealth, State or Territory law will have a clear remedy.

Amendment 155 **Schedule 2, item 120, page 130 (after line 24)**

148. This amendment adds a definition of ‘Ombudsman official’ to subsection 5(1) of the TIA Act. This amendment is consequential to amendment 153. The definition provides that ‘Ombudsman official’ means the Ombudsman, a Deputy Commonwealth Ombudsman, or a person who is a member of the staff referred to in subsection 319(1) of the *Ombudsman Act 1976*.

Amendment 156 **Schedule 2, item 124, page 133 (line 17)**

149. This amendment adds “etc.” to new section 63AB.

Amendment 157 **Schedule 2, item 124, page 134 (after line 23)**

150. This amendment adds subsections (3) – (6) after new subsection 63AB(2).

151. New subsection 63AB(3) states that a person may, in connection with the performance by an Ombudsman official of the Ombudsman official’s functions or duties or the exercise by an Ombudsman official of the Ombudsman official’s powers communicate to the Ombudsman official, make use of, or make a record of, general computer access intercept information.

152. New subsection 63AB(4) states that an Ombudsman official may, in connection with the performance by the Ombudsman official of the Ombudsman official’s functions or duties or the exercise by the Ombudsman official of the Ombudsman official’s powers communicate to another person, make use of, or make a record of, general computer access intercept information.

153. New subsection 63AB(5) states that if information was obtained by intercepting a communication passing over a telecommunications system and the interception was purportedly for the purposes of doing a thing specified in a general computer access warrant and the interception was not authorised by the general computer access warrant then a person may, in connection with the performance by an Ombudsman official of the Ombudsman official’s functions or duties or the exercise by an Ombudsman official of the Ombudsman official’s powers communicate to the Ombudsman official, make use of, or make a record of, that information and an Ombudsman official may, in connection with the performance by the Ombudsman official of the Ombudsman official’s functions or duties or the exercise by the

Ombudsman official of the Ombudsman official's powers communicate to another person, make use of, or make a record of, that information.

154. New subsection 63AB(6) states that 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).

Amendment 158 **Schedule 2, item 124, page 135 (line 24)**

155. This amendment adds "etc." to new section 63AC.

Amendment 159 **Schedule 2, item 124, page 135 (after line 24)**

156. This amendment adds subsections (3) – (6) to section 63AC of the Telecommunications Act.

157. New subsection 63AC(3) states that New subsection 63AC(3) states that a person may, in connection with the performance by an IGIS official of the IGIS official's functions or duties or the exercise by an IGIS official of the IGIS official's powers the IGIS official, make use of[, or make a record of, ASIO computer access intercept information.

158. New subsection 63AC(4) states that An IGIS official may, in connection with the performance by the IGIS official of the IGIS official's functions or duties or the exercise by the IGIS official of the IGIS official's powers communicate to another person, make use of, or make a record of, ASIO computer access intercept information.

159. New subsection 63AC(5) states that if information was obtained by intercepting a communication passing over a telecommunications system and the interception was purportedly for the purposes of doing a thing specified in an ASIO computer access warrant and the interception was not authorised by the ASIO computer access warrant then a person may, in connection with the performance by an IGIS official of the IGIS official's functions or duties or the exercise by an IGIS official of the IGIS official's powers communicate to the IGIS official, make use of, or make a record of, that information and an IGIS official may, in connection with the performance by the IGIS official of the IGIS official's functions or duties or the exercise by the IGIS official of the IGIS official's powers communicate to another person, make use of, or make a record of, that information.

160. 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).

Amendment 160 **Schedule 3, page 154 (after line 16)**

161. This amendment adds section 3SA to the *Crimes Act 1914*. New section 3SA clarifies the relationship of Division 2 of Part IAA of the Crimes Act 1914 to parliamentary privileges and immunities. It provides that Division 2 does not affect the law relating to the powers, privileges and immunities of either House of the Parliament or the members, committees or joint committees of either House of Parliament.

Amendment 161 **Schedule 4, page 166 (after line 2)**

162. This amendment adds section 202B to the *Customs Act 1901*. New section 202B clarifies the relationship of Subdivision C of Division 1 of Part XII of the *Customs Act 1901* to parliamentary privileges and immunities. It provides that Subdivision C does not affect the law relating to the powers, privileges and immunities of either House of the Parliament or the members, committees or joint committees of either House of Parliament.

Amendment 162 **Schedule 5, page 167 (line 30), item 2**

163. This amendment omits subsection 21A(2) and inserts new subsections (2) and (2A) after subsection 21A(1).

164. New subsection 21A(2) states that a request under paragraph (1)(a) may be made orally if the Director-General is satisfied that the request should be made as a matter of urgency or the Director-General is satisfied that making the request in writing would be prejudicial to security or the Director-General is satisfied that making the request in writing would be prejudicial to the operational security of the Organisation.

165. New subsection 21A(2A) states that if subsection (2) does not apply to a request under paragraph (1)(a), the request must be made in writing.

Amendment 163 **Schedule 5, page 168 (after line 5), item 2**

166. This amendment inserts new subsection (3A) after new subsection 21A(3).

167. New subsection 21A(3A) states that if a request is made under paragraph (1)(a), the Director-General must, as soon as practicable, notify the Inspector-General of Intelligence and Security that the request has been made.

Amendment 164 **Schedule 5, page 169 (after line 25), after item 2**

168. This amendment inserts item 2A in Schedule 5 of the Bill to insert subsection (1A) in section 34 of the ASIO Act.

169. New subsection 34(1A) adds to the requirement under section 34(1) regarding the Director-General furnishing to the Attorney-General in respect of each warrant issued under Division 2 of Part 3 a report in writing on the extent to which the action taken under the warrant assisted ASIO in carrying out its functions. Subsection 34(1A) provides that an order was made under subsection 34AAA(2) in relation to the warrant (regarding a person with knowledge of a computer or a computer system to assist access to data – see item 3 of Schedule 5), then the report must also include details of the extent to which compliance with the order has assisted the Organisation in carrying out its functions.

170. Orders under 34AAA are made to access data that is the subject of a warrant under this Division and it is appropriate that warrant reporting also reflect the use of orders connected to a warrant.

Amendment 165**Schedule 5, item 3, page 172 (after line 27)**

171. This amendment amends item 3 of Schedule 5 to the Bill, and inserts subsections 34AAA(3A), (3B), (3C) and (3D). Section 34AAA provides that the Director-General may request the Attorney-General to make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow ASIO to do certain things.

172. Subsection 34AAA(3A) provides that a request under subsection 34AAA(1) can be made either orally or in writing.

173. Subsection 34AAA(3B) provides that, if a request under subsection 34AAA(1) is made orally, the Director-General must make a written record of the request within 48 hours after the request was made.

174. Subsection 34AAA(3C) provides that a request under subsection 34AAA(1) must include a statement setting out the particulars and outcomes of previous requests (if any) relating of the person specified in the current request. This reflects similar requirements on reporting on previous requests for questioning warrants under section 34D of the ASIO Act.

175. Subsection 34AAA(3D) and (3E) provide for the revocation of an under section 34AAA. Subsection 34AAA(3D) provides that if the Director-General is satisfied that the grounds on which an order is made cease to exist, then the Director-General must inform the Attorney-General that the grounds cease to exist. The Director-General must do this as soon as practicable. Subsection 34AAA(3E) provides that the Attorney-General must revoke an order that is in force under section 34AAA where he or she is satisfied that the grounds on which the order was made have ceased to exist.

Amendment 166**Schedule 5, page 172 (after line 35)**

176. This amendment inserts item 4 which creates subsection (1) in section 34ZH of the ASIO Act. This has the effect of moving the existing content of section 34ZH into new subsection 34ZH(1).

177. This amendment inserts item 5 which adds new subsection (2) in section 34ZH of the ASIO Act.

178. New subsection 34ZH(2) states that 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.

Amendment 167**Schedule 5, page 172, at the end of the schedule**

179. This amendment inserts item 6 which adds subsection (2BC) to section 94 of the ASIO Act. Subsection (2BC) provides that a report under subsection (1) must also include a statement of the total number of requests made under paragraph 21A(1)(a) during the period, and the total number of orders made under subsection 34AAA(2) during the period.

180. Section 94 of the ASIO Act sets out the requirements for what must be included in the annual report prepared by the Director-General of Security and given to the Minister under section 46 of the Public Governance, Performance and Accountability Act 2013. A copy of

the annual report must also be given to the Leader of the Opposition in the House of Representatives, and laid before each House of the Parliament within 20 sitting days of that House after the report is received by the Minister.

181. This amendment ensures that Parliament has appropriate oversight of the number of requests for voluntary assistance by ASIO and the number of orders requiring assistance to access data in a given period.