2016 – 2017 – 2018

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

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

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Minister for Home Affairs, the Honourable Peter Dutton MP)

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

GENERAL OUTLINE

1. The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Bill) will amend the *Telecommunications Act 1997* (Telecommunications Act), the *Telecommunications (Interception and Access) Act 1979* (TIA Act), and related legislation, including the *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 introduce measures to better deal with the challenges posed by ubiquitous encryption.

2. Encryption underpins modern information and communications technology. By encoding a message or information so that only authorised parties can access it, encryption protects personal, commercial and government information and promotes confidence in a secure cyberspace. Encryption technologies provide economic benefits by enabling Australians to confidently engage in activities such as online banking and shopping.

3. However, the use of encrypted technologies by terrorists and criminals presents an increasing challenge for law enforcement and national security agencies. Secure, encrypted communications are increasingly being used by terrorist groups and organised criminals to avoid detection and disruption. Over 90% of telecommunications information being lawfully intercepted by the Australian Federal Police now uses some form of encryption. Malicious actors increasingly communicate through secure messaging applications, social media and Voice over Internet Protocol (VoIP) services.

4. The increasing use of encryption has significantly degraded law enforcement and intelligence agencies' ability to access communications and collect intelligence, conduct investigations into organised crime, terrorism, smuggling, sexual exploitation of children and other crimes, and detect intrusions into Australian computer networks. Encryption can conceal the content of communications and data held on devices, as well as the identity of users.

5. Encryption is a global issue, with major technology providers headquartered overseas and communications travelling across national boundaries. Adapting to the challenges of encryption requires international cooperation.

6. National security and law enforcement agencies already work cooperatively with industry and other partners in relation to a range of telecommunications interception matters. The Bill will enhance cooperation by introducing a new framework for industry assistance, including new powers to secure assistance from key companies in the communications supply chain both within and outside Australia (Schedule 1). It will also strengthen agencies' ability to adapt to a digital environment characterised by encryption by enhancing agencies' collection capabilities such as computer access (Schedules 2, 3, 4 and 5).

7. The computer access powers in Schedules 2 to 5 will enable domestic law enforcement agencies to better assist international law enforcement partners by undertaking these powers on behalf of those partners where approved through Australia's mutual assistance framework. These powers recognise the fact that computers, communications and

encryption are now global and perpetrators of crimes and terrorist acts have a global reach through these mediums. This will be based on the principle of reciprocity - that Australia will work with those who work with Australia - and any other conditions the Attorney-General deems appropriate.

8. ***Schedule 1*** introduces a new, graduated approach to industry assistance. The communications industry is in a unique position to assist law enforcement and security agencies in dealing with the challenges posed by encryption. Communications services, software and devices are commonly supplied or operated by entities outside Australia and people frequently communicate across international boundaries. Many people, services and products facilitate the provision of communications and services. For example, the operators of telecommunications networks and application services and the manufacturers of communications devices are supported by entities that enable connectivity across platforms, including cyber security providers and the developers of underlying operating systems. The Bill will enhance cooperation between those providers involved in the communications supply chain and national security and law enforcement agencies. The measures in Schedule 1 will:

- provide a legal basis on which a designated communications provider, including foreign and domestic communications providers and device manufacturers, can provide voluntary assistance under a 'technical assistance request' to the Australian Security Intelligence Organisation (ASIO), Australian Secret Intelligence Service (ASIS), Australian Signals Directorate (ASD) and interception agencies in the performance of their functions relating to Australia's national interests, the safeguarding of national security and the enforcement of the law

- allow the Director-General of Security or the head of an interception agency to issue a 'technical assistance notice' , requiring a designated communications provider to provide assistance that the decision maker is satisfied is reasonable, proportionate, practicable and technically feasible, and

- allow the Attorney-General to issue a 'technical capability notice' , requiring a designated communications provider to do acts or things to ensure the provider is capable of giving help to ASIO and interception agencies where the Attorney-General is satisfied that it is reasonable, proportionate, practicable and technically feasible. The Attorney-General must consult with the affected provider prior to issuing a notice, and may also determine procedures and arrangements relating to requests for technical capability notices.

9. The measures provide financial compensation for assisting agencies, appropriate enforcement mechanisms and immunities from civil liability and specific criminal offences. The Bill maintains the default position that providers assisting government should not absorb the cost of that assistance nor be subject to civil suit for things done in accordance with requests from government.

10. The framework introduced by the Bill operates alongside the existing obligation on domestic carriers and carriage service providers to provide 'such help as is reasonably necessary' to agencies under section 313 of the Telecommunications Act. It will apply to a broader range of providers than are presently captured by that provision, and will allow

national security and law enforcement agencies and the Attorney-General to specify what assistance or capability is required, in consultation with industry.

11. The Bill clearly provides that technical assistance notices and technical capability notices must not require providers to implement or build systemic weaknesses in forms of electronic protection ('backdoors') nor can they prevent providers from fixing an identified weakness or vulnerability. Additionally, the powers in Schedule 1 do not alter a provider's data retention obligations or require a provider to build or retain interception capabilities. These will remain subject to separate, existing legislative arrangements. Access to personal information like telecommunications intercept material, telecommunications content and telecommunications data will continue to require a warrant or authorisation pursuant to existing law.

12. ***Schedule 2*** provides an additional power for Commonwealth, State and Territory law enforcement agencies investigating a federal offence punishable by a maximum of three years imprisonment or more, to obtain covert computer access warrants under the SD Act, similar to those already available to ASIO. The provisions have been aligned with those in the ASIO Act. The schedule also provides for a number of new powers for law enforcement agencies and amendments to the ASIO Act designed to address a range of operational challenges associated with the use of existing computer access powers, including by:

- enabling the interception of communications for the purpose of executing a computer access warrant, removing the need to obtain a second warrant for that purpose

- permitting the temporary removal of a computer or thing from a premises (for example, to a vehicle or nearby premises that has more sophisticated equipment to enable access to the computer), for the purpose of executing a warrant, and to return the computer or thing, and

- enabling agencies to take steps to conceal its access to a computer, following the expiry of the warrant, to address situations where an agency no longer has access to the computer at the time the warrant expires.

13. The offshore storage of information and offshore location of many service providers, makes Australia's mutual assistance framework critical in enabling Australian and foreign authorities access to information to inform investigations and provide admissible evidence for criminal proceedings. Via that framework, foreign authorities will be able to make a request to the Attorney-General to authorise an eligible domestic law enforcement officer to apply for, and execute, a computer access warrant for the purposes of obtaining evidence to assist in a foreign investigation or investigative proceeding. Broadly speaking, this improves the ability of Australian and foreign authorities to work cooperatively, as required, to investigate crimes and acts of terrorism given the international nature of many of these offences.

14. The Bill also updates provisions in the TIA Act which allow security agencies to test their capabilities so that all necessary testing can occur, either independently or with the assistance of a carrier.

15. ***Schedule 3*** will amend the search warrant framework under the Crimes Act to enhance the ability of criminal law enforcement agencies to collect evidence from electronic devices under warrant.

16. The Crimes Act currently allows overt search warrants, which must be made available to the person in relation to a premises, to be issued allowing searches of computers. The amendments in the Bill will allow law enforcement agencies to collect evidence from electronic devices under warrant remotely. That accords with forensic best practice. Law enforcement agencies will be able to execute a warrant in relation to premises or a person without having to be at the premises or in the presence of the person.

17. The Bill also increases the penalties for not complying with orders from a judicial officer requiring assistance in accessing electronic devices where a warrant is in force. The penalty under the Crimes Act will increase from a maximum of two years imprisonment to a maximum five years imprisonment for a 'simple' offence, and up to 10 years imprisonment for contravention of a new 'aggravated' offence (where there is non-compliance with an order related to an investigation into a serious crime). There must be reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device. The current penalty is of insufficient gravity to incentivise compliance with the assistance obligation. The new thresholds represent the maximum penalty that may be imposed and courts retain the discretion to impose a lower penalty in appropriate circumstances.

18. The amendments will also increase the time period during which an electronic device found while executing a warrant can be moved to another place for analysis from 14 days to 30 days to account for the complexity of analysing data in modern electronic communications systems.

19. ***Schedule 4*** will amend the search warrant framework under the Customs Act to enhance the ability of the Australian Border Force (ABF) to collect evidence from electronic devices under warrant in person or remotely. The amendments will provide the ABF with a new power to request a search warrant to be issued in respect of a person for the purposes of seizing a computer or data storage device under the Customs Act.

20. The Bill also increases the penalties for not complying with orders from a judicial officer requiring assistance in accessing electronic devices where a warrant is in force. Penalties for not complying with an order will increase from a maximum six months imprisonment to a maximum five years imprisonment for a 'simple' offence, and up to 10 years imprisonment for an 'aggravated' offence where there is non-compliance with an order related to an investigation into a serious crime. There must be reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device. The current penalty is of insufficient gravity to incentivise compliance with the assistance obligation. The new thresholds represent the maximum penalty that may be imposed and courts retain the discretion to impose a lower penalty in appropriate circumstances.

21. The amendments will also increase the timeframes for the examination of electronic devices moved under a warrant from 72 hours to 30 days to account for the complexity of analysing data in modern electronic communications systems.

22. ***Schedule 5*** provides that, subject to certain limitations, a person or body is not subject to civil liability where they:

- voluntarily provide assistance to ASIO in accordance with a request made by the Director-General, or
- give information or produce a document to ASIO unsolicited (i.e. without a request) if the person or body reasonably believes that it is likely to assist ASIO in the performance of its functions.

23. This Schedule will also enable ASIO to require a person with knowledge of a computer or a computer system to provide assistance that is reasonable and necessary to ASIO in order to gain access to data on a device that is subject to an ASIO warrant. This amendment is an extension of the amendments made in Schedule 3 and 4 which increases the penalties for not complying with orders requiring assistance in accessing electronic devices under the Crimes Act.

ABBREVIATIONS

The following abbreviations will be incorporated throughout this 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)
- *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

24. 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

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

1. This Bill is 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 Bill

2. The Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Bill) will amend the *Telecommunications Act 1997* 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 Bill:

- introduces new provisions that will allow law enforcement and security agencies to secure assistance from key providers in the communications supply chain both within and outside Australia (Schedule 1), and

- enhances agencies' ability to use a range of capabilities, including:

    i. a new power for Commonwealth, State and Territory law enforcement agencies to obtain computer access warrants under the SD Act and enhancements to the computer access warrants already available to ASIO (Schedule 2)

    ii. increased ability of criminal law enforcement agencies to collect evidence from electronic devices under Crimes Act search warrants (Schedule 3)

    iii. a new power for the Australian Border Force (ABF) to request a search warrant to be issued in respect of a person for the purposes of seizing a computer or data storage device (Schedule 4), and

    iv. an enhanced ability for persons to voluntary cooperate with ASIO by providing immunities from civil liability (Schedule 5).

Human rights implications

4. The Bill engages the following human rights:

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

- the right to a fair trial, the right to minimum guarantees in criminal proceedings and the presumption of innocence contained in Article 14 of the ICCPR

- the right to effective remedy contained in Article 2(3) of the ICCPR, and

- protection of the right to freedom of expression contained in Article 19 of the ICCPR.

5. All Schedules of the Bill engage the protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR. Article 17 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. The purpose of the Bill, and the associated limitations on the right to privacy, are to protect national security, public safety, address crime and terrorism. The Bill aims to protect the rights and freedoms of individuals by providing law enforcement and national security agencies with the tools they need to keep Australians safe.

Schedule 1

Protection against arbitrary or unlawful interferences with privacy — Article 17 of the ICCPR

Technical assistance requests and technical assistance notices

8. The provisions that will enable law enforcement, security and intelligence agencies to request assistance (technical assistance request) and compel assistance (technical assistance notice) from designated communications providers (providers) engage the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR. This is because communications providers may facilitate law enforcement, security and intelligence agencies' access to private communications and data where an underlying warrant or authorisation is present.

9. New section 317G of the Telecommunications Act will allow the head of an interception agency, the Director-General of ASIO, the Director-General of the Australian Secret Intelligence Service (ASIS) or the Director-General of the Australian Signals Directorate (ASD) to issue a technical assistance request asking a provider to do specified acts or things. Interception agency includes the Australian Federal Police, Australian Commission for Law Enforcement Integrity, the Australian Criminal Intelligence

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

Commission, State and Territory police forces and State and Territory crime and corruption commissions. A provider who receives a request is not legally required to fulfil the request but may do so voluntarily.

10. New section 317L of the Telecommunications Act will allow the head of an interception agency or the Director-General of ASIO to issue a technical assistance notice where the requirements imposed by the notice are reasonable, proportionate, practicable and technically feasible. Once received, a provider is required to comply with a notice.

11. The assistance that can be requested under a technical assistance request or technical assistance notice must be connected to the activities of a provider and the listed acts or things in new section 317E. This includes providing technical information about a service operated by a provider, assisting with the testing or modification of an agency's internal system or modifying the characteristics of a service. Therefore, any interference with the right to privacy would not arbitrary because a technical assistance request or notice may only be issued for a specified list of acts or things.

12. Under a technical assistance request or technical assistance notice, a provider cannot be asked to provide the content of a communication or private telecommunications data, such as the date, time and duration of a communication without an existing warrant or authorisation under the TIA Act. Subsection 317ZH(1) makes clear that notices have no effect to the extent that they would require a provider to do a thing for which a warrant or authorisation under the TIA Act, the SD Act, the Crimes Act, the ASIO Act, the IS Act or equivalent State and Territory laws would be required.

13. Subsection 317ZH(2) provides that for the purposes of the limitations in subsection 317ZH(1), the Acts referred to are assumed to apply extra-territorially. This means that the limitation under section 317ZH(1) in relation to the need for a warrant or authorisation applies equally to onshore and offshore providers. The head of an agency cannot require an overseas provider to do anything that would require a warrant or authorisation if the provider was a carriage service provider located in Australia. Consequently, the existing legislative schemes will govern how agencies request and receive personal information from all providers. The existing legislative safeguards will continue to apply.

14. For example, the TIA Act prohibits the interception of communications unless a criminal law enforcement agency meets strict statutory thresholds and receives a warrant from a Judge or Administrative Appeals Tribunal (AAT) member. The Judge or AAT member can only issue a warrant if he or she is satisfied that the intercepted information would assist in the investigation of a serious offence (generally offences punishable by at least 7 years – see section 5D of the TIA Act). They are required have regard to the nature and extent of interference with the person's privacy, the gravity of the conduct constituting the offence, the extent to which information gathered under the warrant would be likely to assist an investigation, and other available methods of investigation. The TIA Act also has prohibitions on communicating, using and making records of communications.

15. Where an existing warrant or authorisation under the TIA Act is in place, a notice or request may be issued to facilitate agency access to personal information or communications. For example, a technical assistance notice may ask a provider to decrypt information that would otherwise be unintelligible if the provider has the ability to do so.

16. The Bill pursues the legitimate objective of protecting national security and public order by addressing crime and terrorism. The Bill includes safeguards to protect the right to privacy. The amendments only go so far as is necessary in limiting the right to privacy. Specifically, the assistance requested or compelled must relate to the performance of a function or exercise of a power conferred by law.

17. In the case of a technical assistance notice, an agency head may only issue the notice if satisfied the acts required are reasonable, proportionate, practicable and technically feasible. This means the decision-maker must evaluate the individual circumstances of each notice. The decision-maker must turn his or her mind to the interests of the agency, the interests of the provider, as well as wider public interests, such as the impact on privacy.

18. In determining what is reasonable and proportionate, the decision-maker must have regard to: the interests of national security; the interests of law enforcement; the legitimate interests of the designated communications provider to whom the notice relates; the objectives of the notice; the availability of other means to achieve the objectives of the notice; the legitimate expectations of the Australian community relating to privacy and cybersecurity, and any other matters (if any) that the decision-maker considers to be relevant.

19. The ability to issue a technical assistance request or technical assistance notice is restricted to senior executive staff in all agencies. Accordingly, requests will only be issued by persons with the appropriate seniority and expertise who are in a position to effectively determine the proportionality, reasonableness, practicability and technical feasibility of any request.

20. A technical assistance notice cannot have the effect of requiring a provider to implement or build a systemic weakness or vulnerability into a form of electronic protection. This protection limits the privacy implications of the power by ensuring the security of third parties' communications is not impacted. While systemic weaknesses cannot be built into services or devices, a technical assistance notice can require the selective deployment of a weaknesses or vulnerability in a particular service, device or item of software on a case-by-case basis. Deployment of this kind is necessary to access protected information of suspect individuals and gather intelligence or evidence in the course of an investigation. This will ensure that the powers achieve legitimate, national security and law enforcement objectives without unduly jeopardising the legitimate privacy and information security interests of innocent parties.

21. The measures are permissible limitations on individual privacy. The assistance that agencies may request or compel from providers is not arbitrary as it is prescribed by law. The provisions achieve the legitimate objective of protecting national security and public order. The Bill will assist agencies to fulfil their functions in a digital environment characterised by encryption and enable them to discharge their law enforcement and security functions more effectively. Terrorism, espionage, acts of foreign interference and serious and organised crime are regularly conducted through electronic communication services and devices operated by private providers. Industry is in a unique position to help agencies degrade, disrupt and prosecute criminal activity of this kind.

22. The amendments do not constitute an arbitrary or unlawful incursion into a person's right to privacy. To the extent that there is a restriction on an individual's right to privacy, statutory safeguards ensure any interference is reasonable, necessary and proportionate.

Technical capability notices

23. The new power for the Attorney-General to issue technical capability notices to designated communications providers engages the right to privacy in Article 17 of the ICCPR.

24. To the extent that a person's rights to privacy under Article 17 may be limited, the limitations are reasonable, proportionate and necessary. The power is proportionate and not arbitrary. It is set out in law and subject to a number of safeguards.

25. New section 317T of the Telecommunications Act will allow the Attorney-General to issue a technical capability notice requiring a provider to do acts or things to ensure that the provider is capable of giving help to ASIO or an interception agency.

26. The types of capabilities that may be required to be built under a technical capability notice are limited and must be directed towards ensuring a provider is capable of providing the types of assistance set out in new section 317E or as otherwise determined by the Minister by legislative instrument in 317T(5). Providers cannot be required to build a decryption capability or a capability that removes electronic protection or renders systemic methods of encryption or authentication less effective.

27. Capabilities built under a technical capability notice may assist agencies to access private communications for investigative purposes. However, as discussed above, an existing warrant or authorisation will still be required. The new provisions complement, but do not replace, the existing warrant processes with in-built legislative safeguards.

28. Before issuing a technical capability notice the Attorney-General must be satisfied that the requirements imposed by the notice are reasonable, proportionate and that compliance with the warrant is practicable and technically feasible. This means the Attorney-General must evaluate the individual circumstances of each notice and turn his or her mind to the interests of the agency, the interests of the provider, as well as wider public interests, such as the impact on privacy.

29. In determining what is reasonable and proportionate, the Attorney-General must have regard to: the interests of national security; the interests of law enforcement; the legitimate interests of the designated communications provider to whom the notice relates; the objectives of the notice; the availability of other means to achieve the objectives of the notice; the legitimate expectations of the Australian community relating to privacy and cybersecurity, and any other matters (if any) that the Attorney-General considers to be relevant.

30. Capabilities required under a notice must be related to the established functions of ASIO or an interception agency and related to enforcing the law or safeguarding national security.

31. The power to issue a technical capability notice is limited to the Attorney-General, the highest level of the executive, ensuring direct Ministerial oversight.

32. Prior to a notice being issued, there is a mandatory 28 day consultation period with the relevant provider. This will ensure that the powers are not exercised arbitrarily and give providers an opportunity to make a submission on a notice before having to comply with its requirements. The same obligation to consult applies to a variation of an existing technical capability notice.

33. A technical capability notice cannot require a provider to implement or build a systemic weakness or vulnerability into a form of electronic protection. This includes actions which would make systemic methods of authentication or encryption less effective. This protection limits the privacy implications of the power by ensuring that the Attorney-General cannot require providers to undermine systems that protect the security of personal information. Similar to technical assistance notices, these limitations do not prevent the building of a capability that is able to be deployed selectively to weaken the electronic protection of a particular service, device or item of software.

Use and disclosure of information

34. Information obtained through the new powers will primarily be of a technical nature. Information may include procurement plans, information regarding products and services, network or service design plans and other technical information necessary to execute a request for assistance or to build a capability. Once received, section 317ZF of the Act restricts the ability of agencies to disclose this information without a lawful exception.

35. Strict non-disclosure provisions in 317ZF apply to any information in, or in accordance with, a technical assistance request, technical assistance notice and technical capability notice. Unauthorised disclosure of this information attracts a maximum penalty of imprisonment for five years.

36. To the extent that the information obtained is primarily of a technical nature, the right to privacy is not engaged. However, in the unlikely event that information provided contains information about a person, the prohibition on disclosure without lawful authority promotes the right to privacy. The restrictions on the use and disclosure of information further promote the right to privacy by ensuring any information obtained is only shared for the necessary and legitimate functions of Australian law enforcement, security and intelligence agencies.

37. The measures will not alter the existing framework in the TIA Act for agencies to obtain telecommunications interception information, stored communications and telecommunications data. If an agency receives private information, which was otherwise unintelligible, with the assistance of a notice or request, the range of protections for use and disclosure of this information will apply, including under the TIA Act, Telecommunications Act and *Privacy Act 1988*.

Right to freedom of expression – Article 19 of the ICCPR

Technical assistance requests, technical assistance notices and technical capability notices

38. Article 19(2) of the ICCPR provides that everyone shall have the right to freedom of expression, including the right ‘to seek, receive and impart information and ideas of all kinds

and regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

39. Furthermore, Article 19(3) of the ICCPR provides that the exercise of the rights provided for in Article 19(2) carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary (in part) for the protection of national security or of public order, or of public health or morals.

40. The new measures may engage the right to freedom of expression by indirectly making some people more reluctant to use communications services. It is plausible that a person may minimise their use of communication services if they believe government agencies can ask providers to facilitate access to communications carried through these services, for example by removing forms of electronic protection applied to their communications if they are capable of doing so.

41. However, the amendments will not enable agencies to access communications absent a warrant or authorisation under the TIA Act. Warrants and authorisations under the TIA Act are subject to strict thresholds. For example, interception warrants can generally only be issued to investigate serious offences attracting a maximum penalty of at least 7 years imprisonment.

42. The measures advance a legitimate objective of protecting Australia's national security and public order by allowing law enforcement, security and intelligence agencies to respond to the modern communications environment and effectively access information which will assist investigations and prosecutions.

43. To the extent that a person refrains from or minimises their use of electronic communications in response to these powers, the additional restrictions on the purposes that the powers may be issued for and the limited things that may be required under these powers complement the protections of a warrant and ensure any limitation on the freedom of expression is necessary and proportionate. Additionally, to the extent that the measures do restrict the right to freedom of expression, such a restriction is contemplated by the ICCPR as Article 19(3) allows for restrictions for the protection of national security or of public order.

Right to effective remedy – Article 2(3) of the ICCPR

44. Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights and freedoms recognised by the ICCPR, including the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the State. To the extent that a legal entity subject to a technical capability notice argues that complying with the notice would infringe the rights of natural persons affected by compliance with the notice, the remedies discussed here are applicable.

45. Australian courts will retain jurisdiction for judicial review of a decision of an agency head to issue a technical assistance notice or the Attorney-General's decision to issue a technical capability notice. This will ensure that an affected person, or a provider or behalf of an affected person, has an avenue to challenge unlawful decision making.

46. The Bill does not provide for merits review of decision making and excludes judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act). This approach to review is consistent with similar decisions made for national security and law enforcement purposes – for example those made under the IS Act, ASIO Act, IGIS Act and the TIA Act. Decisions of a law enforcement nature were identified by the Administrative Review Council in its publication *What decisions should be subject to merits review?* as being unsuitable for merits review.

47. Security and law enforcement agencies may require a technical assistance notice in order to access appropriate electronic evidence for an investigation that is underway and evolving. It is imperative that a technical assistance notice can be issued and used quickly. It would not be appropriate for a decision to issue a technical assistance notice to be subject to merits review or judicial review under the ADJR Act, as review could adversely impact the effectiveness and outcomes of an investigation. Decisions by the Attorney-General to issue a technical capability notice are particularly unsuitable for review as they are ministerial decisions to develop law enforcement and national security capabilities.

48. The new industry assistance framework is designed to incentivise cooperation from industry, providing a regime for the Australian government and providers to work together to safeguard the public interest and protect national security. In the unlikely event that enforcement action is required; applications for enforcement under new Division 5 of Schedule 1 will be considered independently by the Federal Court or the Federal Circuit Court.

Schedule 2

Protection against arbitrary or unlawful interferences with privacy — Article 17 of the ICCPR

Amendments to the ASIO computer access warrant to allow limited interception

49. Amendments to the ASIO Act and TIA Act will allow ASIO to intercept communications for the purpose of executing a computer access warrant, removing the need to obtain a second warrant for that purpose.

50. These amendments engage the right to privacy insofar as interception (including interception to enable remote access to a computer) is inherently privacy intrusive. To the extent the right is limited, the limitation is reasonable, necessary and proportionate to the legitimate need for ASIO to have effective powers to execute its statutory function to protect national security.

51. It is almost always necessary for ASIO to undertake limited interception for the purposes of executing a computer access warrant. Currently, ASIO is required to obtain a computer access warrant to gain access to a device and a telecommunications interception warrant under section 9 or 9A of the TIA Act for this interception to establish computer access.

52. The current arrangements cause administrative inefficiency by requiring ASIO to prepare two warrant applications, addressing different legal standards, for the purpose of executing a single computer access warrant. The process requires the Attorney-General to consider each application separately and in accordance with each separate criterion.

53. The amendments will mean ASIO will be able to obtain a single computer access warrant, which authorises an officer to undertake all activities that are required to give effect to that warrant. The amendments enhance the operational efficiency of ASIO to collect intelligence in Australia's interest.

54. The power is proportionate because the new provisions tightly constrain the purposes for which ASIO may use information intercepted under this provision. ASIO can only use intercepted information in order to execute the computer access warrant. In order for ASIO to use intercepted information for its own intelligence value, ASIO must obtain an interception warrant under the TIA Act.

55. Consistent with the existing provisions in the ASIO Act, computer access warrants are subject to strict tests and must be signed by the Attorney-General. The Attorney-General may only issue a warrant if he or she is satisfied that there are reasonable grounds for believing that access to data held in a computer will substantially assist the collection of intelligence in respect of matter that is important in relation to security.

56. The warrant must specify the target computer and premises, as well as the things the warrant authorises.

Amendments to the ASIO computer access warrant to allow temporary removal of a computer

57. Amendments to the ASIO Act will allow ASIO to temporarily remove a computer from a premises for the purpose of executing a computer access warrant. ASIO will not be able to retain the device.

58. Removing a person's device from premises engages the right to privacy because it enables access to devices. ASIO's ability to temporarily remove computers from premises is important in situations where ASIO may require specialist equipment to access the computer. Such equipment may not always be able to be brought onto the premises covertly.

59. As outlined above, statutory safeguards in the ASIO Act protect the right to privacy.

60. The authority to remove a computer is confined to a specific purpose in the warrant. The authority is only available where the Attorney-General has issued a computer access warrant. The Attorney-General must consider the removal of a computer to be appropriate in the circumstances. The Attorney-General may only issue a warrant if he or she is satisfied that there are reasonable grounds for believing that access to data held in a computer will substantially assist the collection of intelligence in respect of matter that is important in relation to security.

61. Oversight of computer access warrants is conducted by the IGIS to ensure the power is exercised lawfully, with propriety and with respect for human rights.

Amendments to the ASIO Act to allow ASIO to take steps to conceal access to a computer

62. Amendments to the ASIO Act will allow ASIO to take steps to conceal its access to a computer following the expiry of a computer access warrant.

63. The amendments engage the right to privacy by enabling ASIO officers to access devices, which hold personal information, for the purposes of concealment.

64. The amendments are necessary to address situations where ASIO no longer has access to the computer at the time the warrant expires but needs to undertake concealment activities. Concealment activities are crucial to ensure that a person does not become aware they are the subject of an investigation, the investigation does not become compromised and sensitive agency capabilities are not revealed.

65. ASIO cannot always reliably predict whether, or when, it will be able to safely retrieve its devices without compromising a covert security intelligence operation. For example, a person may unexpectedly relocate their computer or device prior to the expiry of the warrant, precluding ASIO from taking the necessary steps to conceal the fact that it had accessed the device under warrant until the computer or device is available to be access again.

66. Once the warrant has expired ASIO may not be able to obtain a further computer access warrant to undertake retrieval and concealment activities, as retrieving and concealing would (by definition) not necessarily meet the statutory threshold of 'substantially assisting the collection of intelligence'.

67. The requirement that the concealment activities be performed 'at the earliest time after than 28-day period at which it is reasonably practicable to do so' acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.

68. The authority conferred by the amendments can only be exercised by the Director-General, or a person or class of persons approved by the Director-General in writing. This item provides a safeguard against the arbitrary exercise of the range of activities permitted by the new subsection.

69. Each of the ASIO measures in Schedule 2 is necessary to protect the rights and freedoms of individuals by providing ASIO with the tools it requires to keep Australians safe. To the extent that the right to privacy is limited, the limitation is reasonable, proportionate and necessary to allow ASIO to effectively investigate matters within its statutory remit. The amendments are limited to those which are necessary to address the barriers ASIO faces in using its computer access powers, and are subject to existing statutory protections.

Amendments to the SD Act which grant law enforcement agencies a computer access power, and consequential amendments to the TIA Act

70. Schedule 2 will allow Commonwealth, State and Territory law enforcement agencies to apply for covert computer access warrants under the SD Act. Computer access involves the use of technology to collect information directly from devices, either remotely or physically. This measure engages the right to privacy insofar as accessing a person's personal information held in a computer is inherently privacy intrusive.

71. The measure is directed towards the legitimate purpose of ensuring that law enforcement agencies have appropriate powers to investigate serious crimes. Computer access is a valuable in the current digital environment because it allows officers to access data held on a device in an unencrypted state. The ability to execute computer access

remotely limits interference with property and limits the risk of harm to law enforcement officers.

72. The measure includes a range of safeguards to ensure that the limitation on privacy is reasonable, proportionate and necessary.

73. The law enforcement officer must have reasonable grounds to suspect that access to data held on a particular computer is necessary to investigate a federal offence which carries a maximum penalty of at least three years imprisonment.

74. A Judge or nominated AAT member is responsible for issuing a computer access warrant. In all cases, the Judge or AAT member must have regard to the extent to which the privacy of any person is likely to be affected and the existence of any alternative means of obtaining the evidence or information sought to be obtained.

75. A computer access warrant must specify the things that are authorised under the warrant. The Judge or AAT member must consider whether each thing specified is appropriate in the circumstances. By specifying the types of things authorised in a warrant, there is a limit on the types of things a computer access warrant can enable law enforcement agencies to undertake.

76. A computer access warrant does not authorise the material loss or damage to other persons lawfully using a computer, except where necessary for concealment.

77. The chief officer of the law enforcement agency to which the computer access warrant was issued must revoke the warrant if it is no longer required to obtain evidence of the offence. The chief officer also has an obligation to ensure that access to data is discontinued.

78. The use of information obtained under a computer access warrant is restricted by Division 1, Part 6 of the SD Act. Unauthorised disclosure of information about, or obtained under, a computer access warrant is an offence. The maximum penalty for the offence is two years imprisonment, or 10 years if the disclosure endangers the health or safety of any person or prejudices an investigation into an offence.

79. The use, recording and communication of information obtained in the course of intercepting a communication in order to execute a computer access warrant is also restricted. Where agencies want to gain intercept material for its own purpose, they must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act.

80. The chief officer of a law enforcement agency must report to the Minister on every computer access warrant issued. The report must state whether the warrant or authorisation was executed, the name of the person primarily responsible for the execution, the name of each person involved in accessing data, the name of any person whose data was accessed, and the location at which the computer was located. The report must also give details of the benefit to the investigation.

81. Agencies must report annually on the number of warrants applied for and issued during the year and the number of emergency authorisations.

82. Agencies must keep records about computer access warrants, including in relation to decisions to grant, refuse, withdraw or revoke warrants. Agencies must also keep records of how the information in the warrant has been communicated.

83. The Commonwealth Ombudsman must inspect the records of law enforcement agencies to determine compliance with the law and report the results to the Minister ever six months. The Minister must table Ombudsman reports in the Parliament.

84. These measures are necessary to pursue the legitimate objectives of protecting national security and public order. The amendments address the advances in technology which enable serious criminals to conduct activities and communicate anonymously. To the extent that the right to privacy is limited or interfered with, the interference is appropriate and necessary for law enforcement agencies to effectively investigate and prosecute crime. The limitation to individual privacy is proportionate because the measures are limited to those necessary to meet this legitimate aim and contain strong legislative safeguards.

Amendments to the testing provisions in the TIA Act

85. The Bill amends the testing framework for security authorities in Part 2-4 of the TIA Act to allow security authorities to work with carriers and carriage service providers to test their interception capabilities. Currently, the TIA Act only allows testing by employees of a security authority.

86. The amendments limit the right to privacy to the extent that they provide carriers and carriage service providers with access to intercepted communications.

87. The limitation on privacy is necessary to ensure interception agencies under the TIA Act can effectively test their capabilities which allow them to undertake interception under a warrant. The amendments reflect the practical operation of interception over carrier networks and the people who can effectively assist in testing capabilities.

88. The amendments are subject to a range of safeguards to ensure that, to the extent privacy is interfered with, the interference is reasonable, proportionate and necessary.

89. Security authorities are not able to use information gathered for testing for investigative or intelligence purposes. Information obtained for testing purposes must only be used for testing purposes, and must be destroyed as soon as the purpose for which the information was gathered is no longer applicable. Information gathered for testing purposes may only be exchanged between the relevant carrier/s, a security authority, and interception agencies for the purposes of testing and development.

90. The Attorney-General is responsible for issuing an authorisation to test upon application by a security authority. The amendments will allow carriers to work with security authorities under authorisation, reflecting the practical operation of interception capabilities, and are necessary to pursue the legitimate objectives of protecting national security and public order.

Right to a fair trial, the right to minimum guarantees in criminal proceedings and the presumption of innocence — Article 14 of the ICCPR

91. Article 14 provides (in part) that everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. Additionally Article 14 (3) of the ICCPR provides that in the determination of any criminal charge against him, everyone shall be entitled to certain minimum guarantees including (but not limited to) the right to be informed of the charge and to understand the nature and cause of the charge (14(3)(a)), and to have adequate time and facilities for the preparation of a defence (14(3)(b)). Limiting the right to a fair trial is permissible where it is necessary for the protection of national security and public order and is prescribed by law, and is reasonable, necessary and proportionate in the pursuit of a legitimate objective.

92. Article 14(3)(b) is the right 'to have adequate time and facilities for the preparation of a defence'. The right applies to all stages of the trial and 'facilities' means access to all documents necessary for the defence. Schedule 2 of the Bill engages the right in Article 14(3)(b) by making provision for the protection of computer access technologies and methods in a proceeding. Under section 47A, a person may object to the disclosure of information on the grounds that the information could reveal details of computer access technologies or methods which may be sensitive or reveal capabilities that law enforcement agencies need to keep closely held. The result of section 47A is that there may be circumstances where a defendant will not have a chance to review material that the relevant Judge has decided warrants capability protection.

93. To the extent the right to a fair trial is limited, the limitation is necessary and proportionate. Safeguards include that the presiding officer of the proceeding must make a determination whether the disclosure of the information is necessary for the fair trial of the defendant. It is anticipated that agencies will use computer access powers to gather such material as is necessary to enable other powers to collect evidentiary material, where it is possible to do so. For example, an agency may use a computer access power to gather such intelligence as to enable the application for search warrants under the Crimes Act to be made for a number of suspects. The Crimes Act search warrant would collect such evidence as would be presented in a relevant proceeding. Section 47A does not engage with the right to be informed in detail, in a language the defendant understands, as it only takes effect after charges have been laid.

94. Section 47A(3) provides protection for the right to a fair trial by ensuring that in determining whether or not to make an order not to disclose certain information, the person presiding over the proceeding must take into account whether disclosure of the information is necessary for the fair trial of the defence and whether disclosing it is in the public interest.

95. To the extent that the rights in Article 14 are limited, section 47A of the Bill is a reasonable, necessary and proportionate measure to achieve a legitimate objective. Preventing the release of sensitive operational information into the public domain is essential for the protection of the public and for national security. Releasing such information has inevitable harmful consequences for the ability of law enforcement to conduct future operations.

Schedule 3

Protection against arbitrary or unlawful interferences with privacy — Article 17 of the ICCPR

The power for law enforcement to remotely access computers under the Crimes Act

96. Schedule 3 engages the right to privacy by enabling law enforcement agencies to access private communications and other information on a device using a range of methods. The search warrant framework in the Crimes Act enables law enforcement agencies to search premises and persons, and seize evidential material, in accordance with judicial authorisation. Schedule 3 enhances the ability for executing officers or constables to use electronic equipment, data storage devices and telecommunications facilities in order to obtain access to data held in the computer or device or account based data accessible by the device.

97. Currently under section 3L of the Crimes Act, the executing officer of a warrant in relation to premises or a constable assisting, may operate electronic equipment at the warrant premises to access data if he or she suspects on reasonable grounds that the data constitutes evidential material. To use this power, an officer must be physically located at the warrant premises.

98. These amendments will allow law enforcement agencies to access data without having to physically be on warranted premises. The amendment provides that a warrant in force authorises the officer or assisting constable to use a computer, data storage device found in the course of a search, or a telecommunications facility, or other electronic equipment or a data storage device to obtain data on the computer, or data storage device found in the course of a search to determine whether the data on it is evidential material. The provisions also allow for data to be added, copied, deleted or altered where reasonable to do so. The warrant can be used to access account-based data of a person who is the owner or lessee of the computer, who uses the computer or has used the computer.

99. The Bill includes limitations to ensure that the power is proportionate and does not impact other users of communications services, including joint account holders. Subsection 27E(5) provides that activities undertaken to access data do not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless specified in the warrant. Subsection 27E(5) further provides that activities do not authorise the material loss or damage to other persons lawfully using a computer.

100. The amendments advance the legitimate objectives of protecting national security and public order by providing law enforcement agencies with the tools they require to investigate crimes and protect Australians in a modern context. Interference with privacy is not arbitrary as it is authorised under domestic law. The power for law enforcement to access computers is necessary and proportionate to achieve the legitimate objectives.

Amendments to the Crimes Act which allow criminal law enforcement agencies to compel assistance with accessing devices through a person-based warrant

101. Schedule 3 engages the right to privacy by enabling law enforcement agencies to access private communications and other information on a device held on a person. Under

the current section 3LA of the Crimes Act, law enforcement agencies can compel certain persons (including owners and users of a device) to assist in providing access to data held in, or accessible from, a device that has been seized, moved or found in the course of a search, which has been authorised by a warrant. An order may also require a person to assist in copying data to another device and converting data into an intelligible form. Section 3LA also imposes an obligation, in limited circumstances, upon a person with knowledge of a computer or a computer system to assist access for law enforcement purposes. The current section 3LA predates the existence and common usage of smartphones – it refers to accessing data held in, or accessible from, a computer or data storage device that is on a warrant premises, has been moved from a premises or seized. Those provisions do not envision people carrying smartphones in their pockets.

102. The Bill will resolve this gap by allowing law enforcement agencies to compel persons to assist in providing access to a device under person-based warrant. Inability to access information held on devices may impede legitimate investigations and prosecutions.

103. The amendments in the Bill increase the penalty for a person who commits an offence under this section to five years imprisonment or 300 penalty units from the current penalty of imprisonment of two years, given that this penalty is of insufficient gravity to incentivise compliance with the assistance obligation. The Bill introduces an aggravated offence where a person fails to assist a law enforcement officer to access a device and the offence to which the underlying warrant relates is a serious offence (a Commonwealth offence punishable by imprisonment for two years of more) or a serious terrorism offence. The aggravated offence carries a penalty of 10 years imprisonment or 600 penalty units.

104. Although compelling a person to assist to access a device engages the right to privacy, the limitation is proportionate as a person-based search warrant regime engages the privacy rights of specific persons as opposed to the privacy rights of a wider group of people as does a premises-based warrant.

105. The requirement for a judicial officer to authorise warrants provides an important safeguard for person-based search warrant powers.

106. Before a Judge or AAT member issues a person-based warrant, section 3E(2) of the Crimes Act states that they must be satisfied that there are reasonable grounds for suspecting that the person has in his or her possession, or will within the next 72 hours have in his or her possession, any evidential material. Evidential material is anything relevant to an indictable offence or summary offence that has been or will be committed. A number of additional conditions in Section 3LA(2) must be met before a magistrate grants an order to allow enforcement to compel a person to give assistance accessing data. The person must be connected to the device (for example, as the device owner or user) and have the relevant knowledge to enable them to access the device.

107. The ability to compel assistance is critical to Australia's national security and ensures that law enforcement have the tools necessary to be able to protect Australians. The power for law enforcement to access portable technology devices is necessary and proportionate to achieving the legitimate objectives of protecting national security and public order.

Amendments to the Crimes Act which allow electronic devices moved under warrant to be kept for analysis for 30 days (rather than the current 14 days.)

108. The Bill amends the Crimes Act by extending the timeframes for which a computer or data storage device found in the course of a search may be moved to another location for examination and processing in order to determine whether the computer or data storage device constitutes evidentiary material that should be seized. Moving a person's computer or data storage device engages the right to privacy, as it may restrict a person's access to personal information.

109. Under the current section 3K, a thing moved from a premises must be returned within 14 days, while extensions of no more than seven days may be granted. These amendments will allow a computer or data storage device to be moved for 30 days with an extension of 14 days. These timeframes will allow law enforcement agencies adequate time to conduct the lengthy and intricate forensic processes necessary to determine whether there is evidential material in the electronic device, which may be seized.

110. The amendments achieve a legitimate objective of protecting Australia's national security and public order by ensuring law enforcement can undertake criminal and terrorism investigations in accordance with forensic best practice. The current law does not take into account the length of time that forensic examination of electronic equipment commonly takes.

111. Authorisation of a warrant by a judicial officer will also ensure that movements only occur when necessary and proportionate to meet the legitimate law enforcement and national security objectives. The requirement that the executing officer must believe on reasonable grounds that the computer or data storage device is evidential material, and that the seizure is necessary to prevent the concealment, loss or destruction of that item, provides a limitation on the power. Similarly the requirement that the executing officer must believe on reasonable grounds that the computer or data storage device must be examined to determine whether it constitutes evidentiary material, and movement is necessary to conduct analysis to determine whether the moved item contains or constitutes evidentiary material, provides a limitation on the power. Authorisation by a judicial officer will also ensure that movements and seizures only occur when necessary and proportionate to meet the legitimate law enforcement and national security objectives.

112. Extending the timeframe for examination and processing of computers and data storage devices to 30 days is a proportionate and necessary measure to achieve the legitimate objective of protecting national security and public order.

Schedule 4

Protection against arbitrary or unlawful interferences with privacy — Article 17 of the ICCPR

The power for the Australian Border Force to search persons who may have computers or storage devices under the Customs Act

113. Schedule 4 engages the right to privacy by enabling a judicial officer to issue a warrant authorising the ABF to search or frisk search a person if the judicial officer is satisfied that there are reasonable grounds for suspecting that the person possesses, or will

possess in the next 72 hours, a computer or data storage device that is evidential material. Evidential material is anything relevant to an indictable offence or summary offence. Under existing laws, the ABF could only obtain a judicial warrant to search premises. The amendments recognise that information is often stored on devices, held physically by persons, and that an inability to access this information may impede legitimate investigations and prosecutions.

114. While the nature of searching a person in order to gain access to a device is inherently intrusive, it is not arbitrary as it is a targeted law enforcement tool designed to assist the ABF to effectively investigate crimes in the current technological environment. The power has the legitimate objective of protecting national security and public order.

115. The requirement for a judicial officer to authorise warrants will provide an important safeguard for the new power of the ABF. Under the amendments, there is a strict time limit of seven days to undertake a search authorised by the warrant. To the extent that the right to privacy is limited or interfered with, the interference is proportionate and necessary to meet legitimate objectives.

The power for the Australian Border Force to remotely access computers under the Customs Act

116. Schedule 4 engages the right to privacy by enabling the ABF to access private communications and other information on a device using a range of methods. Amendments to the search warrant framework in the Customs Act will enable the ABF to use electronic equipment, data storage devices and telecommunications facilities where a search warrant is in force in order to obtain access to data held in the computer or device or account based data accessible by the device.

117. At present, under section 201 of the Customs Act, the executing officer of a warrant in relation to premises or a person assisting, may operate electronic equipment at the warrant premises to access data if he or she believes on reasonable grounds that the data constitutes evidential material. To use this power, an officer must be physically located at the warrant premises.

118. New subsection 199(4A) and 199B(2) will allow the ABF to access data without having to physically be on warranted premises. The amendments provide that a warrant in force authorises the officer or assisting person to use a computer, data storage device found in the course of a search, or a telecommunications facility, or other electronic equipment or a data storage device to obtain data on the computer, or data storage device found in the course of a search to determine whether the data on it is evidential material. The provisions also allow for data to be added, copied, deleted or altered where reasonable to do so. The warrant can be used to access account-based data of a person who is the owner or lessee of the computer, who uses the computer or has used the computer.

119. The Bill includes limitations to ensure that the power is proportionate and does not impact other users of communications services, including joint account holders. The addition, deletion or alteration of data is not authorised when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless specified in the warrant. The addition, deletion or alteration of data is also not authorised when those actions are likely to cause any other material loss or damage to other persons lawfully using a computer.

120. The amendments pursue the legitimate objectives of protecting national security and public order by providing the ABF with the tools they require to investigate criminal activity and protect Australian's national security in a modern context. Interference with privacy is not arbitrary as it is authorised under domestic law. The power for ABF to access computers is necessary and proportionate to achieving the legitimate objectives.

The power for the Australian Border Force to move a computer or data storage device in the course of a search under a warrant pursuant to the Customs Act

121. Schedule 4 engages the right to privacy by enabling a person-based search warrant to authorise the movement of a computer or data storage device in the course of a search to another location in order to determine whether the computer or data storage device constitutes evidentiary material that should be seized. The executing officer must believe on reasonable grounds that the computer or device is evidential material in relation to an offence to which the warrant relates, and the movement is necessary to prevent its concealment, loss or destruction or its use in committing an offence. These amendments reflect the current provisions for premises-based search warrants in the Customs Act, which allow an executing officer to move evidential material or suspected evidential material found on a premises.

122. This power will allow the ABF to analyse the computer or data storage device for evidence, enhancing their ability to conduct investigations and assist prosecutions. Any limitation or interference with the right to privacy is necessary and in the interests of law enforcement and national security.

123. Authorisation of a warrant by a judicial officer will also ensure that movements only occur when necessary and proportionate to meet the legitimate national security and public order objectives. The requirement that the executing officer must believe on reasonable grounds that the computer or data storage device is evidential material, and that the seizure is necessary to prevent the concealment, loss or destruction of that item, provides a limitation on the power. Similarly the requirement that the executing officer must believe on reasonable grounds that the computer or data storage device must be examined to determine whether it constitutes evidentiary material, and movement is necessary to conduct analysis to determine whether the moved item contains or constitutes evidentiary material, provides a limitation on the power. Authorisation by a judicial officer will also ensure that movements and seizures only occur when necessary and proportionate to meet the legitimate objectives.

Amendments to the Customs Act which allows the Australian Border Force to compel assistance with accessing data held in devices that have been seized or moved under a person-based search warrant

124. Schedule 4 engages the right to privacy by enabling the ABF to access private communications and other information on a device held on a person. The amendments will enable a magistrate to issue an order requiring a specified person to provide access to data held in, or accessible from, a computer or data storage device that has been seized, moved or found in the course of a person-based search, which has been authorised by a warrant. An order may also require a person to assist in copying data to another data storage device and converting data into an intelligible form. A similar order, requiring a person to provide access to data held in a computer on a warrant premises, is available under the Customs Act.

125. The amendments in the Bill increase the penalty for a person who does not provide access to a computer or device to five years imprisonment or 300 penalty units from the current penalty of imprisonment of two years, given that this penalty is of insufficient gravity to incentivise compliance with the assistance obligation. The Bill introduces an aggravated offence where a person fails to assist a law enforcement officer to access a device and the offence to which the underlying warrant relates is a serious offence or a serious terrorism offence. The aggravated offence carries a penalty of 10 years imprisonment or 600 penalty units.

126. These amendments will assist the ABF to access information within a computer or data storage device, which may otherwise be inaccessible or unintelligible. They are designed to assist the ABF in their investigations, particularly in the areas of national security and organised crime.

127. The requirement for a magistrate to authorise warrants provides an important safeguard for person-based search warrant powers. To grant an order, the magistrate must be satisfied of a number of things set out in the legislation, including that: there are reasonable grounds for suspecting that evidential material is held in, or accessible from, the computer or device; that the person is connected to the computer or device (for example, as the owner or user); and that the person has relevant knowledge to enable access to data held in, or accessible from, the computer or device.

128. To the extent these amendments limit the right to privacy, the interference would be reasonable, necessary and proportionate to achieving the legitimate objectives of protecting national security and public order.

Amendments to the Customs Act which allow computers or storage devices moved under warrant or found in the course of a search authorised by a warrant to be kept for examination or processing for 30 days (rather than the current 72 hours.)

129. The Bill also includes amendments to timeframes for how long a device may be moved for analysis. Moving a person's computer or data storage device engages the right to privacy, as it may restrict a person's access to personal information.

130. Under the current section 200 of the Customs Act, a thing moved from premises must be returned within 72 hours. These amendments will extend the time period for moved computers and data storage devices to 30 days and allow time extensions of 14 days. These timeframes will allow the ABF adequate time to conduct the lengthy and intricate forensic processes necessary for electronic devices.

131. The amendments achieve a legitimate objective of protecting Australia's national security and public order by ensuring the ABF can fulfil its statutory functions with forensic best practice.

Schedule 5

132. Schedule 5 enables ASIO to require a person with knowledge of a computer or a computer system to provide assistance that is reasonable and necessary to ASIO in order to gain access to data on a device that is subject to an ASIO warrant. A person commits an offence if he or she does not comply with an order where capable of doing so. The maximum penalty is 5 years imprisonment.

133. The types of assistance that ASIO may seek under these amendments include compelling a target or a target's associate to provide the password, pin code, sequence or fingerprint necessary to unlock a phone.

134. This measure engages the right to privacy by assisting ASIO to access private communications and other information on a person's device. Legislative safeguards ensure any limitation on the right to privacy is reasonable and proportionate.

135. ASIO must seek an order from the Attorney-General to require a person to provide assistance. The Attorney-General must be satisfied that the device is subject to an issued ASIO warrant. This means that the thresholds of the particular warrant have been met. For example, under a computer access warrant, access to data must substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security.

136. The person who is to be given the order must also be reasonably suspected of being involved in activity prejudicial to security, or a person who is otherwise connected to the device. The person must also have relevant knowledge of the device or computer network.

137. The measures are directed towards the legitimate objective of ensuring that ASIO can give effect to warrants which authorise access to a device. ASIO's inability to access a device can frustrate operations to protect national security. The measures are a reasonable and proportionate response to the challenges brought about by new technologies, including encryption.

Conclusion

138. This Bill is compatible with human rights and promotes a number of human rights. To the extent that the Bill limits a human right, those limitations are reasonable, necessary and proportionate.

NOTES ON CLAUSES

Preliminary

Item 1 – Short title

1. This item provides for the short title of the Act to be the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

Item 2 – Commencement

2. This item provides for the commencement of each provision in the Bill, as set out in the table. Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

3. Schedule 1 of the Bill is to commence on a single day fixed by Proclamation. However, if the provisions do not commence within the period of nine months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.

4. Schedule 2, Parts 1 and 2 and Schedules 3, 4 and 5 are to commence the day after this Act receives the Royal Assent.

5. Schedule 2, Part 3 is to commence the later of a) immediately after the commencement of Schedule 2, Part 1 or b) immediately after the commencement of Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018.* If the events of paragraph b) do not occur then Schedule 2, Part 3 is not to commence.

Item 3 – Schedules

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

Schedule 1 – Industry assistance

Administrative Decisions (Judicial Review) Act 1977

Item 1 – After paragraph (daaa) of Schedule 1

7. Item 1 inserts new paragraph (daaaa) into Schedule 1 of the ADJR Act to include decisions under new Part 15 of the Telecommunications Act as decisions to which the ADJR Act does not apply.

8. Judicial review under the ADJR Act will not be available for decisions made by the Director-General of ASIO, the head of an interception agency or the Attorney-General under new Part 15. These decisions will deal with highly sensitive information relevant to agency capabilities or ongoing investigations and will involve matters of high policy importance, like national security, where judgments are best made by the executive arm of government. Judicial review will be available through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of section 39B(1) of the *Judiciary Act 1903*.

Criminal Code Act 1995

9. Amendments to the Criminal Code are necessary to ensure providers are not criminally responsible for particular telecommunications and computer offences for any acts or things done consistent with a technical assistance request, technical assistance notice or technical capability notice issued under new Part 15 of the Telecommunications Act.

Item 2 - After subsection 474.6(7) of the Criminal Code

10. Item 2 inserts new subsection 474.6(7A) into the Criminal Code to ensure persons are not criminally responsible for an offence against subsection 474.6(5) of the Criminal Code if the conduct of the person is in accordance with a technical assistance request, or in compliance with a technical assistance notice or technical capability notice.

11. This item extends the existing exemption from criminal responsibility under subsection 474.6(7) of the Criminal Code, which provides that law enforcement officers, or intelligence or security officer acting in good faith in the course of his or her duties do not commit an offence where the conduct of the person is reasonable in the circumstances for the purpose of performing that duty.

12. A person will not commit an offence under subsection 474.6(5) if the person, in accordance with a technical assistance request, technical assistance notice or technical capability notice, uses or operates any apparatus or device (whether or not it is comprised in, connected to or used in connection with a telecommunications network), and this conduct results in hindering the normal operation of a carriage service supplied by a carriage service provider.

13. In accordance with subsection 13.3(3) of the Criminal Code, a defendant will bear the evidential burden under new subsection 474.6(7A).

Item 3 - After subparagraph 476.2(4)(b)(iii) of the Criminal Code

14. Item 3 amends the meaning of unauthorised access, modification or impairment for the purposes of Part 10.7 of the Criminal Code, which contains computer offences. These offences prohibit a person from 'causing' unauthorised access, modification or impairment to:

a. access data held in a computer; or

b. modification of data held in a computer; or

c. the impairment of electronic communication to or from a computer; or

d. the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means.

15. Subsection 476.2(3) of the Criminal Code makes clear that a person causes unauthorised access, modification or impairment if the person's conduct substantially contributes to it. Subparagraphs 476.2(4)(b)(i) – (iii) create a number of exceptions to the prohibition, including causing access, modification or impairment under a warrant issued under the law of the Commonwealth, a State or Territory.

16. Item 3 further adds to these exceptions to ensure that a person will not commit an offence contained in Part 10.7 if the person, acting in accordance with a technical assistance request or in compliance with a technical assistance notice or technical capability notice does certain acts or things that substantially contributes to access, modification or impairment of the types of things in 476.2. Although the powers in new Part 15 cannot authorise access, modification or impairment in circumstances where a warrant or authorisation would be required (new section 317SC of Part 15 makes this clear), there may be circumstances in which things done consistent with a technical assistance request, technical assistance notice or technical capability notice substantially contribute to access, modification or impairment under a warrant or otherwise.

Item 4 - Dictionary in the Criminal Code

17. Item 4 inserts definitions into the Criminal Code dictionary for technical assistance notice, technical assistance request and technical capability notice. The item provides that these terms have the same meaning as in Part 15 of the Telecommunications Act.

Telecommunications Act 1997

Item 5 – Section 7

18. Item 5 inserts the definition of ASIO into the Telecommunications Act.

Item 6 – Section 7 (paragraph (a) of the definition of civil penalty provision)

19. Item 6 amends the definition of civil penalty provision to exclude new section 317ZB.

20. New section 317ZB establishes a separate penalty provision for designated communications providers apart from the existing provisions in Telecommunications Act.

Item 7 – After Part 14

21. Item 7 inserts new Part 15 into the Telecommunications Act.

Part 15 – Industry assistance

Division 1 – Introduction

New Part 15 of the Telecommunications Act is divided into eight Divisions. Division 1 provides an outline of Part 15 and defines a number of key terms

317A – Simplified Outline of this Part

22. New section 317A provides a simplified outline of new Part 15. It briefly describes the frameworks for technical assistance requests, technical assistance notices and technical capability notices.

317B - Definitions

23. New section 317B provides the definition for many of the terms which have a particular meaning under Part 15, as follows:

a. ***access*** is defined as including access subject to a pre-condition (such as the use of a password), access by way of push technology and access by way of standing request. Push technology involves access that is not initiated by an end-user (pull technology).

b. ***ASIO affiliate*** has the same meaning as in section 4 of the ASIO Act. The definition captures persons performing functions or services for ASIO but it does not include the Director-General or an ASIO employee.

c. ***ASIO employee*** has the same meaning as in section 4 of the ASIO Act. The definition captures persons employed by the Director-General for the performance of ASIO's functions and the exercise of ASIO's powers.

d. ***chief officer*** of an interception agency has the meaning given by new section 317ZM.

e. ***contracted service provider*** in relation to a designated communications provider is defined as persons who perform services for or on behalf of a provider. It does not include employees of the provider.

f. ***Corruption and Crime Commission (WA)*** means the Corruption and Crime Commission established by the *Corruption, Crime and Misconduct Act 2003* (WA).

g. ***designated communications provider*** is defined under new section 317C. This definition is further elaborated upon below.

h. ***electronic service*** is defined under new section 317D. This definition is further elaborated upon below.

i. ***eligible activities*** of a designated communications provider is provided for in new section 317C. This definition is further elaborated upon below.

j. ***entrusted ASD person*** is defined as a person who:

   i. is a staff member of ASD; or
   ii. has entered into a contract, agreement or arrangement with ASD; or
   iii. is an employee or agent of a person who has entered into a contract, agreement or arrangement with ASD.

k. ***entrusted ASIO person*** has the same meaning as in section 4 of the ASIO Act. This means:
   i. an ASIO employee; or
   ii. an ASIO affiliate; or
   iii. a person who has entered into a contract, agreement or arrangement with ASIO.

l. ***entrusted ASIS person*** means a person who:

   i. is a staff member or agent of ASIS; or
   ii. has entered into a contract, agreement or arrangement with ASIS; or
   iii. is an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIS.

m. ***giving help*** is defined in relation to the agencies that are able to receive help by way of a technical assistance request, technical assistance notice or technical capability notice. When used in relation to ASIO, '*giving help*' includes giving help to an ASIO affiliate or ASIO employee: that is, someone performing functions or services for ASIO under the ASIO Act; or someone employed by the Director-General under the ASIO Act. When used in relation to ASIS, '*giving help*' includes giving help to a staff member of ASIS. When used in relation to ASD, '*giving help*' includes giving help to a staff member of ASD. When used in relation to an interception agency, '*giving help*' includes giving help to an officer of the agency.

n. ***IGIS official*** has the same meaning as in section 4 of the ASIO Act. The definition captures the Inspector-General of Intelligence and Security and members of staff employed by the Inspector-General to perform functions and exercise powers under the IGIS Act.

o. ***Independent Broad-based Anti-corruption Commission of Victoria*** is defined as the Independent Broad-based Anti-corruption Commission established by the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic).

p. ***Independent Commissioner Against Corruption (SA)*** means the person appointed Commissioner under section 8 of the Inde*pendent Commissioner Against Corruption Act 2012 (SA*).

q. ***interception agency*** is defined as any of the below:

i. the Australian Federal Police; or
ii. the Australian Commission for Law Enforcement Integrity; or
iii. the Australian Crime Commission; or
iv. the Police Force of a State or the Northern Territory; or
v. the Independent Commission Against Corruption of New South Wales; or
vi. the New South Wales Crime Commission; or
vii. the Law Enforcement Conduct Commission of New South Wales; or
viii. the Independent Broad-based Anti-corruption Commission of Victoria; or
ix. the Crime and Corruption Commission of Queensland; or
x. the Independent Commissioner Against Corruption (SA); or
xi. the Corruption and Crime Commission (WA).

These are the same agencies which have powers to intercept live communications under a warrant issued by a Judge or AAT member pursuant to the TIA Act.

r. ***Law Enforcement Conduct Commission of New South Wales*** means the Law Enforcement Conduct Commission constituted by the *Law Enforcement Conduct Commission Act 2016 (NSW).*

s. ***listed act or thing*** is provided for in new section 317E. This definition is further elaborated upon below.

t. ***material*** is defined broadly to include material whether in the form of text, data, speech, music, other sounds or visual images (moving or otherwise). It also includes material in any other form or any combination of forms.

u. ***member of the staff of the Independent Commissioner Against Corruption (SA)*** means a person who is engaged under subsection 12(1) of the *Independent Commissioner Against Corruption Act 2012* (SA).

v. ***officer***, when used in relation to an interception agency, has the same meaning given by new section 317ZM.

w. ***staff member***, when used in relation to ASIS or ASD has the same meaning as in the IS Act. Section 3 of that Act states that staff member in relation to an agency is a member of the staff of the agency (including employees, consultants or contractors or seconded persons from other Commonwealth or State authorities).

x. ***supply***, when used in relation to a facility, customer equipment or a component, is defined as including the supply (and re-supply) by way of sale, exchange, lease, hire or hire-purchase. Supply, when used in relation to software, includes provide, grant or confer rights, privileges or benefits.

y. ***technical assistance notice*** means a notice given under new section 317L.

z. ***technical assistance notice information*** is defined broadly to include information about any of the following:

i. the giving of a technical assistance notice;
ii. the existence or non-existence of a technical assistance notice;
iii. the variation of a technical assistance notice;
iv. the revocation of a technical assistance notice;
v. the requirements imposed by a technical assistance notice; or
vi. any act or thing done in compliance with a technical assistance notice.

It also includes any other information about a technical assistance notice.

aa. ***technical assistance*** request means a request under new paragraph 317G(1)(a). This concept is further elaborated upon below.

bb. ***technical assistance request information*** is defined broadly to include information about any of the following:

i. the giving of a technical assistance request
ii. the existence or non-existence of a technical assistance request;
iii. the acts or things covered by a technical assistance request; or
iv. any act or thing done in accordance with a technical assistance request.

It also includes any other information about a technical assistance request.

cc. ***technical capability notice*** means a notice given under new section 317T. This concept is further elaborated upon below.

dd. ***technical capability notice information*** is defined broadly to include information about any of the following:

i. the giving of a technical capability notice;
ii. consultation relating to the giving of a technical capability notice;
iii. the existence or non-existence of a technical capability notice;
iv. the variation of a technical capability notice;
v. the revocation of a technical capability notice;
vi. the requirements imposed by a technical capability notice;
vii. any act or thing done in compliance with a technical capability notice; or
viii. any other information about a technical capability notice.

317C – Designated communications provider etc.

24. The table in new section 317C defines ***designated communications provider*** and ***eligible activities*** for the purposes of new Part 15. The designated communications providers set out in column 2 of items 1 – 15 of the table include key participants in the global communications supply chain. The eligible activities set out in column 2 against each item establish their relevant functions for the purposes of new Part 15.

25. Designated communications providers (hereafter provider) are entities which can be given a technical assistance request made under new section 317G, a technical assistance notice made under new section 317L or a technical capability notice made under new section 317T. Designated communications providers are defined in the table in section 317C to include the full range of participants in the global communications supply chain, from carriers to over-the-top messaging providers. This reflects the multi-layered nature of the communications environment and the types of entities that could meaningfully assist law enforcement and national security agencies.

26. It is crafted in technologically neutral language to allow for new types of entities and technologies to fall within its scope as the communications industry evolves.

27. Requests under new section 317G, or requirements under new sections 317L and 317T must be connected to one or more of the eligible activities of a designated communications provider. The categories of designated communications provider are drafted to ensure a connection to Australia. This geographical nexus enables Australian agencies to request assistance from offshore entities that have, or are likely to have, a key role in the provision of communications and related services in Australia, whilst limiting the power to Australia's jurisdictional limits.

28. New section 317C captures instances where a product or service is manufactured with default settings and shipped globally – that is, it is not exclusively or specifically intended for use in Australia - but is likely to be used in Australia.

29. Individuals, as well as body corporates, may be designated communications providers. A person may fit into one or multiple categories in the table in section 317C.

30. The eligible activities of a designated communications provider are activities to which technical assistance requests, technical assistance notices and technical capability notices must relate.

31. Item 1 of the table lists carriers or carriage service providers. Carriers and carriage service providers are defined in the Telecommunications Act. A carrier is an entity that owns a telecommunications network unit that supplies carriage services to the public. Carriage service providers use a telecommunications network unit to supply carriage services to the public. Carriage services include services for carrying communications. For example, telephone services, internet access service and VoIP services. As owners or operators of telecommunications network units used to supply carriage services, carriers must hold a licence issued by the Australian Communications and Media Authority.

32. Item 2 of the table lists carriage service intermediaries. Carriage service intermediaries are defined in the Telecommunications Act. Carriage service intermediaries

are legal persons who arrange for the supply of carriage services by a carriage service provider to a third party.

33. Item 3 of the table lists persons that provide a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service. This provision is designed to ensure that other persons that have a significant role in the supply of carriage services and the passage of communications through carriage services may be asked or required to provide assistance.

34. Item 4 of the table lists persons that provide an electronic service that has one or more end-users in Australia. '*Electronic service*' is defined in new section 317D and means a service that allows end-users to access material using a carriage service, or a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service. For the purposes of item 4 a person must provide the electronic service to one or more end-users in Australia.

35. Item 5 of the table lists persons that provide a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia. This provision is designed to ensure that other persons that have a significant role in the provision of electronic services may be asked or required to provide assistance to Australian authorities.

36. Item 6 of the table lists persons that develop, supply or update software used, for use, or likely to be used, in connection with a listed carriage service or an electronic service that has one or more end-users in Australia. This category would include, for example, persons involved in designing trust infrastructure used in encrypted communications or software utilised in secure messaging applications.

37. Item 7 of the table lists persons that manufacture, supply, install, maintain or operate a facility. *Facility* is defined in the Telecommunications Act and means any part of the infrastructure of a telecommunications network or any line, equipment, apparatus, tower, mast, antenna, tunnel, duct, hole, pit, pole or other structure or thing used, or for use, in or in connection with a telecommunications network.

38. Item 8 of the table lists persons that manufacture or supply components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia. Equipment in the telecommunications network can be highly technical and comprised of multiple components.

39. Item 9 of the table lists persons that connect a facility to a telecommunications network in Australia, including mesh networks, private networks and entities involved in the provision of undersea cables.

40. Item 10 of the table lists persons that manufacture or supply customer equipment for use, or likely use, in Australia. Customer equipment is defined in section 21 of the Telecommunications Act and includes any equipment, apparatus, structure, thing or system that is used or ready for use or intended for use on the customer side of the boundary of a telecommunications network. Section 22 of that same Act establishes the boundary of a telecommunications network. The persons in item 10 include suppliers and manufacturers of mobile devices, modems and computing devices typically connected to the telecommunications network.

41. Item 11 of the table lists persons that manufacture or supply components for use, or likely use, in the manufacturer of customer equipment for use, or likely use, in Australia. This includes persons who manufacturer circuit boards, subscriber identification modules (SIMs) or memory units of a mobile device.

42. Item 12 of the table lists persons that install or maintain customer equipment in Australia in a capacity other than that of an end-user of the equipment. This includes technical experts or contractors installing or maintaining customer equipment provided by a manufacturer, supplier or retailer, such as managed service providers. Persons with ongoing maintenance obligations, or persons acting at the point of installation, are able to provide essential assistance in the course of an investigation.

43. Item 13 of the table lists persons who connect customer equipment to a telecommunications network in Australia in a capacity other than that of an end-user of the equipment. This includes systems integrators.

44. Item 14 of the table lists constitutional corporations that manufacturer, supply, install or maintain data processing devices for use, or likely use, in Australia. *Data processing device* is defined in section 7 of the Telecommunications Act and means any article or material from which information is capable of being reproduced, with or without the aid of any other article or device. A data processing device may not necessarily be connected, or designed to be connected, to the telecommunications network. Item 14 includes persons who maintain data storage centres or manufacturer discrete storage devices.

45. Item 15 of the table lists constitutional corporations that develop, supply or update software that is capable of being installed on computer or other equipment that is, or is likely to be, connected to a telecommunications network in Australia. This includes persons who develop application software or system software (including operating systems) that may be installed on a computer in Australia such as personal computers or mobile devices.

317D - Electronic service

46. Under section 317C (items 4 and 5), a person who provides an ***electronic service***, or a service that facilitates, or is ancillary or incidental to, the provision of an electronic service, is a designated communications provider.

47. New section 317D defines *electronic service* to mean a service that allows end-users to access material using a carriage service, or a service that delivers material to persons having equipment appropriate for receiving that material (see definition in section 317B), where the delivery of the service is by means of a carriage service. The definition is designed to be capable of capturing a range of existing and future technologies, including hardware and software. Examples of electronic services may include websites and chat fora, secure messaging applications, hosting services including cloud and web hosting, peer-to-peer sharing platforms and email distribution lists, and others. The inclusion of the carriage service requirement in the definition of electronic service provides the nexus between the new offence and the telecommunications head of legislative power in subsection 51(v) of the Constitution.

48. The definition does not extend to a broadcasting service or datacasting service (within the meaning of the *Broadcasting Services Act 1992*).

49. By virtue of new subsection 317D(2), a service includes a website.

50. ***Material*** is defined in new section 317B and includes material in the form of text, data, speech, music or other sounds, visual images (moving or otherwise) or material whether in any other form or combination of forms.

51. New subsections 317D(3) and 317D(4) stipulate that a person does not provide an electronic service merely because the person supplies a carriage service that enables material to be accessed or delivered or because the person provides a billing service, or a fee collection service, in relation to an electronic service. Suppliers of carriage services are excluded from the definition of electronic service because their obligations are explicitly captured in items 1 – 3 of the table in 317C.

52. New subsection 317D(5) makes clear that a reference in this section to the use of a thing is a reference to the use of the thing either in isolation or conjunction with one or more other things.

317E - Listed acts or things

53. New section 317E inserts the definition of *listed acts or things* for the purposes of new Part 15.

54. Technical assistance requests and technical assistance notices may contain the listed acts or things in section 317E(1) but additional forms of assistance of a similar kind may also be specified in the technical assistance request or technical assistance notice. In contrast, technical capability notices must be directed towards ensuring a provider can give the types of assistance set out in section 317E(1) – with the exception of 317E(1)(a) which does not apply to technical capability notices. That is, 317E(1)(b) – (j) is exhaustive with respect to technical capability notices and non-exhaustive with respect to technical assistance requests and technical assistance notices. Additional types of capabilities may only be developed if set out in a legislative instrument determined by the Minister in accordance with subsection 317T(5).

55. The different application of 317E identifies the distinction between circumstances where a provider is already capable of giving assistance and circumstances where a provider might be required to build a capability so that they become capable of giving assistance. The powers in Part 15 are intended to be exercised flexibly to request or compel forms of assistance that a provider is already capable of giving, so long as it is of a similar kind or nature as the things specified in 317E. However, in cases where a provider is required to build a capability that goes beyond its own needs, the matters for which this capability can be built are limited in the legislation and subject to ongoing Parliamentary scrutiny.

<u>317E(1)(a)</u>

56. New paragraph 317E(1)(a) lists removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider, as an act or thing that may be specified. Although agencies may specify removing electronic protection in a technical assistance request and technical assistance notice, agencies may not require providers to build a capability to remove electronic protection under a technical capability notice (see 317T(4)(c)(i)).

57. Removing one or more forms of electronic protection is intended to include decrypting encrypted communications. Requirements to decrypt or remove electronic protection under this subsection cannot oblige a provider to furnish the content or metadata of private communications to authorities. Consistent with the restrictions in new section 317ZH, agencies must access communications content and data through established warrants and authorisations under the TIA Act. However, if the content or data obtained under such a warrant is encrypted, the Director-General of ASIO or the chief officer of an interception agency could issue a technical assistance notice under new section 317L requiring a provider to assist with decryption where the provider is capable of doing so.

317E(1)(b)

58. New paragraph 317E(1)(b) lists providing technical information as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. Technical information could include information about the design, manufacture, creation or operation of a service, the characteristics of a device, or matters relevant to the sending, transmission, receipt, storage or intelligibility of a communication. Examples include source code, network or service design plans, and the details of third party providers contributing to the delivery of a communications service, the configuration settings of network equipment and encryption schemes. It could also include providing demonstrations of technologies. Technical information does not include telecommunications data such as subscriber details or the source, destination or duration of a communication for which an authorisation under the TIA Act would be required.

59. Obligations to provide technical information apply regardless of whether the information is subject to intellectual property rights or contractual arrangements. Immunity from civil liability for any acts or things done in accordance (or in good faith purportedly in accordance) with a technical assistance request, technical assistance notice and technical capability notice will be available to persons that provide assistance.

60. Consistent with the decision-making criteria for technical assistance notices in section 317P and technical capability notices in section 317V, the decision-maker must evaluate the individual circumstances surrounding each notice in order to determine whether the provision of particular technical information is reasonable and proportionate. Some kinds of technical information are more sensitive than others, such as source code. It is incumbent on the decision-maker to consider whether it is appropriate to specify source code, having regard to the commercial interests of the provider and whether other technical information, or other kinds of assistance, could achieve a similar law enforcement or national security objective.

317E(1)(c)

61. New paragraph 317E(1)(c) lists installing, maintaining, testing or using software or equipment as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice.

62. Assistance of a kind contemplated by 317E(1)(c) includes installing, maintaining, testing or using software or equipment given to a provider by, or on behalf, of an agency. The deployment of agency procured or developed software or equipment within an existing network owned or operated by a provider can achieve law enforcement objectives without imposing on the providers to develop technology secondary to their core business.

63. Requirements to install software are subject to the global protections against building or implementing a systemic weakness in a form of electronic protection in 317ZG. Accordingly, a provider could not be required to install or utilise any agency software or equipment that weakens security across non-target devices or services.

317E(1)(d)

64. New paragraph 317E(1)(d) lists ensuring information obtained in connection with the execution of a warrant or authorisation is given in a particular format as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. Assistance of this kind includes reformatting data, providing information to authorities consistent with prescribed templates, ensuring information can be delivered in an appropriate and efficient manner and other obligations relating to the intelligibility of material obtained through a warrant or authorisation.

317E(1)(e)

65. New paragraph 317E(1)(e) lists facilitating or assisting access to the following things that are the subject of the eligible activities of a provider as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice:

i. a facility
ii. customer equipment
iii. a data processing device
iv. a listed carriage service
v. a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service
vi. an electronic service
vii. a service that facilitates, or is ancillary or incidental to, the provision of an electronic service
viii. software used, for use, or likely to be used, in connection with a listed carriage service
ix. software used, for use, or likely to be used, in connection with an electronic service, and
x. software that is capable of being installed on a computer, or other equipment, that is, or is likely to be connected to a telecommunications network.

66. Access includes physical or online access. The terms *facility*, *customer equipment*, *data processing device* and *listed carriage service* are defined in the Telecommunications Act. *Electronic service* is defined in new section 317D and means a service that allows end-users to access material using a carriage service, or a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service.

67. Access to the things listed above can assist agencies where they have developed a technical solution but require help from providers to implement it, or where providers are

able to modify their systems (without creating a systemic weakness) to assist the execution of a warrant or authorisation to access information held on the above things.

68. For the purposes of new subsection 317E(1)(e) access includes physical or online access.

69. Agencies cannot ask a provider to put their staff at risk when facilitating assistance of this kind under new subsection 317E(1)(e). It is not reasonable or proportionate to require civilians to undertake hazardous activities in the context of a law enforcement or security agency investigation.

317E(1)(f)

70. New paragraph 317E(1)(f) lists assisting with the testing, modification, development or maintenance of a technology or capability as an act or thing that may be specified in a technical assistance request, technical assistance notice and technical capability notice. Assistance consistent with this paragraph includes help testing, modifying, developing or maintaining the internal systems and capabilities of law enforcement and security agencies. Providers can ensure that agency systems are compatible with the networks, services or devices they manufacture, supply and operate. When expert providers and agencies collaborate to deploy agency capabilities the chances of efficient and effective deployment significantly increase.

71. Assistance of this kind is particularly helpful to agencies seeking to install or maintain equipment on a provider's network consistent with new paragraph 317E(1)(c).

317E(1)(g)

72. New paragraph 317E(1)(g) lists notifying particular kinds of changes to, or developments affecting, eligible activities of the provider, if the changes are relevant to the execution of a warrant or authorisation, as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. The changes that may be notified include, but are not limited to, offering new or improved services or products, outsourcing arrangements, offshoring equipment or services, changes to services, procuring new equipment or changes to the management of services.

73. This item is limited to changes that may impact a particular warrant or authorisation. It is not uncommon for a particular application or service to receive multiple daily updates. Given the frequency of change and the commercial sensitivity of some updates, this item is limited to instances where the change would affect a warrant or authorisation on foot. By way of example, an agency may seek notification of changes to a specific service that a target is using in the context of a specific investigation. Notification of these changes will allow the agency to take steps to mitigate its impact before it occurs.

317E(1)(h)

74. New paragraph 317E(1)(h) lists modifying, or facilitating the modification of, any of the characteristics of a service provided by the provider as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice. By way of example, modification of a service could include blocking the delivery of a specific service to a target.

317E(1)(i)

75. New paragraph 317E(1)(i) lists substituting, or facilitating the substitution of, a service provided by the provider for additional services as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice.

76. As with assistance under 317E(1)(e), agencies cannot ask a provider to put their staff at risk. It is not reasonable or proportionate to require civilians to undertake hazardous activities in the context of a law enforcement or security agency investigation.

317E(1)(j)

77. New paragraph 317E(1)(j) lists doing an act or thing to conceal the fact that anything has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory as an act or thing that may be specified in a technical assistance request, technical assistance notice or technical capability notice.

78. In the course of an investigation law enforcement and security agencies often need to exercise covert powers to gain evidence and intelligence about the activities of targets. The disclosure of these activities can jeopardise an investigation and prejudice the interests of law enforcement and national security agencies.

79. Assistance of a kind described in paragraph 317E(1)(j) includes doing acts or things to ensure that a target does not become aware they are the subject of an investigation, minimising the risk that the investigation becomes compromised or that sensitive agency capabilities are revealed.

80. A technical assistance request, technical assistance notice or technical capability notice can only seek assistance of this kind if it is connected to a valid function or power conferred by law that relates to the legitimate purposes of enforcing the criminal law and laws imposing pecuniary penalties, assisting enforcement of the criminal laws in force in a foreign country or if the purpose is in the interests of Australia's national security, foreign relations or economic well-being. This ensures any activity a provider is asked to conceal is legitimate and consistent with the proper conduct of an agency as established by law.

81. New paragraph 317E(2) ensures that providers cannot be asked to make false or misleading statements or engage in dishonest conduct for the purposes of 317E(1)(j). Providers have obligations to their customers as well as Government. Subsection 317E(2) confirms that providers cannot be asked to actively deceive a person for the purposes of concealing lawful agency activities.

317F – Extension to external Territories

82. New subsection 317F makes clear that this Part extends to every external Territory.

Division 2 – Voluntary technical assistance

83. Division 2 sets out the framework for the heads of ASIO, ASIS, ASD and interception agencies to request voluntary technical assistance from designated communications providers. A request from voluntary technical assistance is known as a technical assistance

request. Immunity from civil liability for any acts or things done in accordance with a technical assistance request will be available to persons that provide assistance in accordance with this Division. Agency heads may enter into contractual agreements with providers relating to the provision of assistance

317G - Voluntary technical assistance provided to ASIO, ASIS, ASD or an interception agency

84. New section 317G specifies the circumstances under which a provider gives voluntary technical assistance for the purposes of Part 15.

85. New subsection 317G(1) establishes protection from civil liability for, or in relation to, acts or things done by providers, and any officer, employee or agent of the provider, in accordance, or in good faith purportedly in accordance, with a voluntary technical assistance request.

86. Section 317G allows the Director-General of Security, the Director-General of ASIS, the Director-General of ASD or the chief officer of an interception agency to give a voluntary technical assistance request to a provider to do things that are in connection with the eligible activities of the provider. This means that assistance under this framework is limited to the technical functions of a provider set out in the table in section 317C.

87. A technical assistance request can ask a provider do a thing currently within their capacity, or request that they build a new capability to assist agencies. Both forms of assistance are entirely voluntary in nature and must be consistent with the powers and functions of the requesting agency.

88. The persons who can make technical assistance requests occupy the most senior position in their organisation and can exercise suitable judgment about the propriety of such a request, and the relevant terms of any contract – particularly whether it is appropriate to extend civil immunity for acts or things done consistent with the request or whether public resources should be spent on contracting with a provider under this Division. New sections 317ZN, 317ZP, 317ZQ and 317ZR allow agency heads to delegate these powers to senior officials in their organisations, who are also equipped to make these judgments.

89. The civil immunity established in the new section protects providers that assist law enforcement, security and intelligence agencies. For example, if a provider is asked to give details of the development of a new service or technology, they should not be liable for any breach of intellectual property rights.

90. Providers have immunity from civil liability for things done in accordance, or in good faith purportedly in accordance, with a voluntary technical assistance request. For example, if a provider is asked to give details of the development of a new service or technology, they will not be liable for any breach of intellectual property rights. The provision of civil immunity is similar to protections under subsection 313(5) of the Telecommunication Act for carriers and carriage service providers that do things in order to meet their obligations under that section to provide reasonably necessary help to law enforcement and national security agencies. It is full immunity for civil actions brought under Commonwealth law.

91. New subsection 317G(5) makes it clear that things requested of a provider must be for the purpose of helping the relevant agency perform functions or powers conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

a. enforcing the criminal law and law imposing pecuniary penalties; or

b. assisting the enforcement of the criminal laws in force in a foreign country; or

c. the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

92. This is consistent with the purposes for which agencies currently seek assistance from domestic carriers and carriage service providers under section 313 of the Telecommunications Act.

93. The things may also include matters that facilitate, or are ancillary or incidental to, an agency's performance of a function or exercise of a power where the function or power relates to the above purposes. This will allow things necessary for the smooth execution of a request to be specified.

94. The things that may be specified in a technical assistance request include, but are not limited to, the listed acts or things set out in section 317E. Other types of assistance may be specified in a technical assistance request provided that the assistance is of the same kind, class or nature as those listed.

Terms

95. The term '*conferred by or under a law'* in new subparagraph 317G(2)(b)(v) means that the function or power may be conferred by legislation or a legislative instrument made under a power delegated by the Parliament. For example, the function or power may be conferred by a regulation made under an Act of Parliament.

96. The meaning of '*enforcing the criminal law'* for the purposes of new subparagraph 317G(5)(a) includes the process of investigating crime and prosecuting criminals. It also includes precursory and secondary intelligence gathering activities that support the investigation and prosecution of suspected offences. The term 'criminal law' includes any Commonwealth, State or Territory law that makes particular behaviour an offence punishable by fine or imprisonment.

97. The reference to '*pecuniary penalties'* in new subparagraph 317G(5)(a) relates to penalties for breaches of Commonwealth, State and Territory laws that are not prosecuted criminally or that impose a penalty which serves as an administrative alternative to prosecution (often referred to as civil or administrative penalty provisions). Pecuniary penalties for the purposes of this provision are not intended to encompass small-scale administrative fines. In Commonwealth, State and Territory legislation there are significant pecuniary penalties for serious breaches of the law, particularly laws regarding corporate misconduct.

98. The inclusion of '*assisting the enforcement of the criminal laws in force in a foreign country'* in new subparagraph 317G (5)(b) will ensure that technical assistance requests can be made in support of Australia's international obligations such as those under Council of

Europe Convention on Cybercrime or the MACMA. For example, requests may be made to facilitate the disclosure of stored communications to foreign law enforcement agencies, where the disclosure is also supported by a stored communications warrant under the TIA Act.

99. The reference to Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being in new subparagraph 317G(5)(d) reflects the functions of Australia's intelligence and security agencies as set out in the IGIS Act and the ASIO Act. It is intended to support voluntary technical assistance requests made by Australia's intelligence and security agencies. It is not intended to support voluntary assistance requests made by interception agencies.

100. New subsection 317G(6) states that the acts or things that may be specified in a technical assistance request include, but are not limited to, the listed acts or things set out in new section 317E. Other types of assistance may be specified in a technical assistance request provided that the assistance is of the same kind, class or nature as those listed.

101. New paragraphs 317G(6)(a) and 317G(6)(b) require these listed acts or things to be connected to the eligible activities of the provider as set out in new section 317C and must be covered by the requirements described in new subsection 317G(2).

317H - Form of technical assistance request

102. New section 317H specifies that a technical assistance request must be given in writing, although oral issue is permissible in urgent circumstances. If issued orally, a written record is must be made within 48 hours of the request and then, as soon as practicable, a copy must be given to the provider.

317HAA – Provision of advice to designated communications providers

103. New subsections 317HAA(1)-(4) requires 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. The purpose of this provision is to clarify that compliance with a technical assistance request is voluntary.

317HA – Duration of technical assistance request

104. New section 317HA specifies that a technical assistance request comes into force when given, or when specified in the request. Requests only remain in force until the expiry date specified in the request, or in cases where no expiry date was specified, at the end of 90 days after issue.

317J - Specified period etc.

105. New section 317J specifies that a technical assistance request may include a request that a specified act or thing be done in a specified period of time, or specified manner, or in a way that meets one or more specified conditions. Subsection 317J(3) makes clear that this section does not limit subsections 317G(1) and (2).

106. This section reflects the distinction between the specific acts or things that may be asked of a provider in accordance with 317G and the manner in which those things should be executed. For example, a law enforcement agency may request that a provider remove security controls from a particular device consistent with 317E(1)(a) and, additionally, request that these controls be removed in a short timeframe to assist with an urgent operation.

317JA - Variation of technical assistance requests

107. New section 317JA allows the issuer of a technical assistance request to make variations to the request.

108. The issuer of a technical assistance request must make variations to the request in writing. Oral variation is permissible in urgent circumstances but must be followed by a written copy.

109. Any acts or things specified in a varied technical assistance request must be connected to the eligible activities of a provider and connected to helping the agency perform a function or exercise a power conferred by law, so far as the function or power relates to:

a. enforcing the criminal law and law imposing pecuniary penalties; or

b. assisting the enforcement of the criminal laws in force in a foreign country; or

c. the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

110. New subsection 317JA(9) requires that any acts or things specified in a varied technical assistance request must be connected to the eligible activities of a provider and covered by the requirements in 317G(2). New subsection 317JA(10) provides that the things that may be specified in a varied technical assistance notice include, but are not limited to, the listed acts of things in new section 317E.

317JB - Revocation of technical assistance requests

111. New section 317JB allows the issuer of a technical assistance request to revoke the request. Revocation must be in writing to the person to whom the request was given.

317K - Contract etc.

112. New section 317K provides authority for the relevant agency head to enter into arrangements with a provider in relation to acts or things done by the provider in accordance with a technical assistance request. This section provides a statutory basis for Commonwealth, State and Territory agencies to enter into contracts, including contracts of a financial nature, for the purposes of Division 2.

Division 3 – Technical assistance notices

113. Division 3 allows the Director-General of Security, or the chief officer of an interception agency to give a provider a technical assistance notice requiring them to do specified acts or things within the notice, where they are already capable of doing so. A provider issued with a notice is obliged to comply with the requirements set out in the notice.

114. Anything required by a notice must be related to the functions or powers of an agency conferred by law and relevant to enforcing the law or safeguarding national security.

115. Notices may be issued where a provider is unable or unwilling to provide assistance to law enforcement and security agencies in the manner required, absent a legal obligation.

317L – Technical assistance notices

116. New section 317L allows the Director-General of Security, or the chief officer of an interception agency, to give a provider a technical assistance notice requiring the provider to do things in connection to the eligible activities of the provider in new section 317C and the things that are covered by new subsection 317L(2).

117. Technical assistance notices may require a provider to give assistance to ASIO or an interception agency in relation to the performance of that agency's functions or powers. The acts or things specified in a notice will be limited to forms of assistance a provider is already capable of giving. For example, a technical assistance notice may require a provider to assist with the decryption of material lawfully intercepted under a warrant if their systems enable them to decrypt this material; it could not however require a provider to build a new decryption capability.

118. The power to issue technical assistance notices is reserved for agency heads in the first instance. Persons occupying these senior positions are able to exercise judgement about the propriety of requiring a provider to comply with the acts or things specified in a notice. New sections 317ZN, 317ZP, 317ZQ and 317ZR allow agency heads to delegate these powers to senior officials in their organisations who are also equipped to make these judgements.

119. New subsection 317L(2) makes it clear that the specified acts or things in a notice must be done for the purpose of helping the relevant agency perform functions or powers conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

a. enforcing the criminal law and laws imposing pecuniary penalties; or

b. assisting the enforcement of the criminal laws in force in a foreign country; or

c. safeguarding national security.

120. The specified acts or things may also go to matters that facilitate, or are ancillary or incidental to, the agency's performance of a function or exercise of a power where the function or power relates to these purposes. This will allow things necessary for the smooth execution of a notice to be set as requirements.

121. The terms in new paragraph 317L(2)(c) have the same meaning as they do for technical assistance requests made under new section 317G.

122. New subsection 317L(3) states that the acts or things that may be specified in a technical assistance notice include, but are not limited to, the listed acts or things set out in new section 317E. Other types of assistance may be specified in a technical assistance notice provided that the assistance is of the same kind, class or nature as those listed. That assistance

must also be connected to the eligible activities of the provider and related to the agencies functions.

123. New paragraphs 317L(3)(a) and 317L(3)(b) require these listed acts or things to be connected to the eligible activities of the provider as set out in new section 317C and must be covered by the requirements described in new subsection 317L(2).

317M – Form of technical assistance notice

124. A technical assistance notice must be given in writing, although oral issue is permissible in urgent circumstances. If issued orally, a written record is must be made within 48 hours of issue and then, as soon as practicable, a copy must be given to the provider.

317MAA – Provision of advice to designated communications providers

125. New subsections 317MAA(1)-(2) requires the Director-General of Security, or the chief officer of an interception agency to advise a designated service provider of their obligations to comply with a technical assistance notice if they have been issued with a notice. The obligations to comply with a notice provided in section 317ZA for carriers and carriage service providers, and section 317B for designated communications providers (other than carriers and carriage service providers). This provision ensures that providers understand their obligations in either 317ZA or 317ZA so far as they relate to the technical assistance notice.

317MA – Duration of technical assistance notice

126. New section 317MA provides that a technical assistance notice comes into force when given or when specified in the notice. Notices only remain in force until the expiry date specified in the notice, or in cases where no expiry date was specified, at the end of 90 days after issue.

317N – Compliance period etc.

127. New section 317N specifies that a technical assistance notice may require that a specified act or thing be done in a specified period of time, or specified manner, or in a way that meets one or more specified conditions. This section operates in a manner consistent with new section 317J.

128. This section reflects the distinction between the specific acts or things that may be required from a provider in accordance with 317L and the manner in which those things should be executed. For example, a law enforcement agency may request that a provider remove security controls from a particular device consistent with 317E(1)(a) and, additionally, request that these controls be removed in a short timeframe to assist with an urgent operation.

317P - Decision-making criteria

129. New section 317P inserts a requirement that, before giving a technical assistance notice, the Director-General of Security or the chief officer of an interception agency must be satisfied that the requirements imposed by the notice are reasonable and proportionate, and compliance with the notice is practicable and technically feasible.

130. Satisfaction for the purposes of this section is a subjective state of mind of the administrative decision maker. [2] It is a precondition to the exercise of a power. To meet the requisite state of satisfaction the decision-maker must consider the reasonableness and proportionality of the requirements imposed by the notice and the practicability and technical feasibility of compliance with that notice. The decision-maker's satisfaction must be formed on a correct understanding of the law.[3] The decision-maker must not take into account a consideration which a court can determine in retrospect 'to be definitely extraneous to any objects the legislature could have had in view.'[4]

131. This means the decision-maker must evaluate the individual circumstances of each notice. In deciding whether a notice is reasonable and proportionate, it is necessary for the decision-maker to consider both the interests of the agency and the interests of the provider. This includes the objectives of the agency, the availability of other means to reach those objectives, the likely benefits to an investigation and the likely business impact on the provider. It is important that the provider is the most appropriate person to provide the assistance sought by the agency. For example, a notice given to a provider who, while able to assist, did not control the relevant data and was not in a position to help as adequately as a more directly related provider would not be proportionate. In that instance it would need to be clear that the controller of the data was unable to assist.

132. The decision-maker must also consider wider public interests, such as any impact on privacy, cyber security and innocent third parties. In deciding whether compliance with the notice is practicable and technically feasible, the decision-maker must consider the systems utilised by a provider and provider expertise. To be satisfied, the decision-maker would need to consider material information given to the agency by the provider. It is expected that the agency would be engaged in a dialogue with the provider prior to issuing a notice. The decision-maker may also make inquiries with other persons who have relevant experience and technical knowledge.

133. These provisions are designed to ensure that providers cannot be required to comply with excessively burdensome or impossible assistance measures. For example, if the decision-maker cannot be satisfied that it is technically feasible to remove a form of electronic protection due to the technical aspects of how that electronic protection is deployed, the decision-maker could not issue a notice containing such a requirement. These conditions also ensure that the decision-maker must be satisfied that a notice will not impose an impracticable regulatory burden or have a disproportionate impact on the business activities of a provider.

317Q – Variation of technical assistance notices

134. New section 317Q allows the Director-General of Security or the chief officer of an interception agency to vary a technical assistance notice that has been given to a provider. Variations must be made in writing. Oral variation is permissible in urgent circumstances but must be followed by a written copy.

[2] *R v Anderson; Ex parte Ipec-Air Pty Ltd* (1965) 113 CLR 177 at 189; [1965] HCA 27 citing *Sharp v Wakefield* [1891] AC 173 at 179.
[3] *Minister for Immigration and Multicultural Affairs v Eshetu* (1999) 197 CLR 611 at 651-654.
[4] *Water Conservation and Irrigation Commission (NSW) v Browning* (1947) 74 CLR 492 at 505.

135. New subsection 317Q(8) requires that any acts or things specified in a varied technical assistance notice must be connected to the eligible activities of a provider and covered by the requirements in 317L(2) , so far as the function or power relates to:

d. enforcing the criminal law and law imposing pecuniary penalties; or

e. assisting the enforcement of the criminal laws in force in a foreign country; or

f. safeguarding national security.

136. New subsection 317Q(9) provides that the things that may be specified in a varied technical assistance notice include, but are not limited to, the listed acts of things in new section 317E.

137. New subsection 317Q(10) requires the Director-General of Security or the chief officer of an interception agency must not vary a notice unless satisfied that the requirements imposed are reasonable and proportionate and compliance with the varied notice is practicable and technically feasible.

138. These provisions ensure that the power to vary a notice is exercised consistently with the power to issue a notice and any varied requirements are within the bounds of what might have been required of a technical assistance notice at first instance.

317R – Revocation of technical assistance notices

139. New section 317R allows the Director-General of Security or the chief officer of an interception agency to revoke a technical assistance notice in writing to the person to whom the notice was given.

140. New subsections 317R(2) and 317R(4) requires the Director-General of Security or the chief officer of an interception agency to revoke a technical assistance notice if satisfied that the acts or things specified in the notice are not reasonable and proportionate or that compliance with the warrant is not practicable and technically feasible. Changing business requirements, developments in technology or shifts in the operational priorities of agencies may render the acts or things specified in a notice inconsistent with these statutory requirements. The revocation provision establishes an avenue to discontinue notices that have become obsolete or excessively burdensome.

317RA – Whether requirements imposed by a technical assistance notice are reasonable and proportionate

141. New section 317RA requires that, in determining whether a technical assistance notice or a varied technical assistance notice is reasonable and proportionate the decision maker must have regard to the following matters:

a. the interests of national security;

b. the interests of law enforcement;

c. the legitimate interests of the designated communications provider to whom the notice relates;

d. the objectives of the notice;

e. the availability of other means to achieve the objectives of the notice;

f. the legitimate expectations of the Australian community relating to privacy and cybersecurity; and

g. any other matters (if any) that the Director-General of Security or the chief officer considers to be relevant.

Division 4 – Technical capability notices

142. Division 4 allows the Attorney-General to issue a technical capability notice that is directed towards ensuring that the designated communications provider is capable of giving listed help to ASIO or an interception agency. However, a technical capability notice cannot be used to compel a provider to build a capability that would enable it to remove encryption, or any form of electronic protection, from products. The things specified in technical capability notices may require significant investment. The capabilities built under a technical capability notice may be utilised by multiple agencies. This is distinct from assistance required by a technical assistance notice under new section 317L which can oblige a provider to give help that they are already capable of providing to the requesting agency.

143. For administrative efficiency, technical capability notices, which have more stringent consultation and approval requirements, can also be used to compel a provider to give help as can be required under a technical assistance notice. It would create unnecessary red tape for a separate technical assistance notice to be required to compel assistance in relation to a capability that had been developed pursuant to a technical capability notice.

144. Requirements in a notice must be related to the functions or powers of ASIO or an interception agency and relevant to enforcing the law or safeguarding national security. A provider is obliged to comply with the requirements set out in the notice.

317S – Attorney-General may determine procedures and arrangements relating to requests for technical capability notices.

145. New section 317S enables the Attorney-General to set the parameters for requests by government agencies to issue a technical capability notice. This includes establishing administrative processes to centralise agency requests, or compartmentalise arrangements to protect requests of a sensitive nature. Acts or things done under technical capability notices may support the functions of multiple agencies and procedures established under new section 317S may also ensure that additional agencies are notified of requests being made, facilitating the efficient sharing of capabilities developed under a notice.

146. New subsection 317S(2) provides that a determination made by the Attorney-General under subsection 317S(1) may require that the agreement of a person or body must be obtained before a request is made for a technical capability notice.

147. New subsection 317S(3) provides that a failure to comply with a determination made by the Attorney-General under subsection 317S(1) does not affect the validity of a technical capability notice.

148. New subsection 317S(4) makes clear that a determination under subsection 317S(1) is not a legislative instrument. The determination is administrative rather than legislative in character. A determination does not determine or alter the law but instead explains how the law will be administered.

317T – Technical capability notices

149. New section 317T allows the Attorney-General to give a provider a technical capability notice requiring a provider to do one or more specified acts or things that are in connection to the eligible activities of the provider and are covered by new subsection 317T(2). This has the effect of limiting the assistance required by a warrant to the technical functions of a provider set out in new section 317C.

150. The power to issue technical capability notices is reserved for the Attorney-General. This ensures that the power to require a provider to build a capability, beyond that which it already has, is restricted to the highest levels of government and directly subject to Ministerial oversight.

151. Things specified in a warrant must, consistent with paragraph 317T(2)(a), be directed towards ensuring that the provider is 'capable of giving ***listed help'*** to the relevant agency, or in accordance with paragraph 317T(2)(b), be by way of giving help to the relevant agency (or both). Accordingly, conditions within a technical capability notice may:

a. Require a provider to do something that will ensure it is capable of giving assistance, and/or

b. Require a provider to give assistance it is already capable of giving.

152. The term 'capable of giving ***listed help*****'** goes to the capability requirements in the notice. It allows the Attorney-General to require a provider to do acts or things that will enable a provider to give ***listed help*****.** The term ***listed help*** is defined in new subsection 317T(4) and includes the matters set out in section 317E. New section 317E applies exhaustively to ***listed help*** under this section and requirements to build capabilities must go towards ensuring a provider is capable of providing the forms of assistance set out in new paragraphs 317(1) (b) – (j).

153. ***Listed help*** also includes a matter that is determined by legislative instrument under new subsection 317T(5). New subsection 317T(5) allows the relevant Minister to determine one or more kinds of things for the purposes of new subparagraph 317T(4)(c)(ii). This legislative instrument making power allows the Minister to list further areas with respect to which capabilities under a notice may be built, additional to the listed acts or things in 317E. In accordance with section 19 of the *Acts Interpretation Act 1901*, the Minister refers to the Minister, or any of the Ministers, administering this provision of the Act. The communications industry is one of the world's most dynamic industries and it is important that law enforcement and security agencies retain the ability to combat crime and national security threats notwithstanding advances in technology.

154. New subsection 317T(6) provides that before the Minister makes a determination under new subsection 317T(5) to add additional items to the things a capability can be made for, he or she must have regard to:

a. the interests of law enforcement,

b. the interests of national security,

c. the objects of the Telecommunications Act,

d. the likely impact of the determination on designated communications providers, and

e. any other relevant matter (if any) as the Minister considers relevant.

155. These considerations will ensure that any legislative instrument put before Parliament has been drafted with the needs of both Government, industry and the public in mind. To satisfy the conditions it is expected that the Minister will consult with industry before tabling an instrument.

156. Requirements within a notice set in accordance new paragraph 317T(2)(b) go to acts of assistance that a provider is already capable of giving. This means agencies will not need to seek two different notices, with different issuing persons, in order to require a provider to build a capability and then use that capability to give the agency help. It will also be possible for an agency to require a provider to provide immediate help while, or before, it builds a capability for the agency. It is appropriate for technical capability notices to have this dual function given that they have more stringent consultation and approval requirements than technical assistance notices. It would create unnecessary red tape for a separate technical assistance notice to be required to compel assistance in relation to a capability that had been developed pursuant to a technical capability notice.

157. New subsection 317T(7) makes clear that the acts or things done under a technical capability notice which are by way of giving this type of help to a relevant agency include (but are not limited to) the matters set out in new section 317E. Accordingly, the listed acts or things in new section 317E do not limit the forms of assistance that may be requested from a provider, if the provider already has the capacity to give this assistance. Other types of assistance may be specified in a technical capability notice outside of the matters in 317E so long as it of same kind, class or nature as those listed and is by way of giving help to a relevant agency.

158. Any specified acts or things in a notice must be done for the purpose of helping the relevant agency perform functions or powers conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to a relevant objective listed in new subsection 317T(3). The specified acts or things may also help the relevant agency in a matter that facilitates, or is ancillary or incidental to, that agency's performance of a function or exercise of a power where the function or power relates to a relevant objective.

159. New subsection 317T(3) defines ***relevant objective*** for the purposes of section 317T as:

a. enforcing the criminal law and laws imposing pecuniary penalties; or

b. assisting the enforcement of the criminal laws in force in a foreign country; or

c. safeguarding national security.

160. The meaning of these terms is consistent with their meaning in new subsection 317L(2).

161. New subsection 317T(8) provides that a technical capability notice has no effect to the extent to which it requires a provider to ensure a telecommunications service or telecommunications system has:

a. a capability to enable a communication passing over the system to be intercepted

b. a capability to transmit lawfully intercepted information to applicable delivery points, or

c. a delivery capability.

162. Interception capabilities are dealt with in Parts 5-3 of the TIA Act. Delivery capabilities are dealt with in Part 5-5 of that same Act.

163. Delivery capability means the capability of a telecommunications service or system to enable lawfully intercepted information to be delivered to interception agencies. The TIA Act imposes on carriers and carriage service providers obligations to develop, install and maintain interception and delivery capabilities. Technical capability notices issued under 317T will not extend these obligations to additional categories of providers or qualify the nature of the existing obligations on carriers and carriage service providers. For example, a technical capability notice cannot be issued to require an offshore provider not subject to current interception obligations in Part5-3 of the TIA Act to build a capability that directly causes the provider to intercept communications passing through its system. Likewise, a technical capability notice cannot be issued to impose requirements on a carrier or carriage service provider that go specifically to their existing obligations under Part 5-3 of the TIA Act. Capabilities of this type will continue to be regulated through established statutory regimes.

164. New subsection 317T(9) makes it clear that for the purposes of subsection (8), ensuring that a kind of service or a system has a particular capability includes ensuring that the capability is developed, installed and maintained.

165. New subsection 317T(10) provides that a technical capability notice cannot require a provider to build and/or maintain a data retention capability. This includes retaining the categories of information in section 187AA of the TIA Act. The retention of telecommunications data is managed through a separate statutory scheme in Part 5-1A of that Act. This provision ensures that technical capability notices cannot be used to extend the scope of providers subject to a data retention capability.

166. New subsection 317T(11) provides that any expression used in subsection (7), (8) or (9) has the same meaning as in Chapter 5 of the TIA Act. Ensuring conformity between the relevant provisions in this Act and the relevant provisions in the TIA Act provides additional surety that technical capability notices cannot modify, or qualify in any way, legislated obligations on providers in relation to interception capabilities, delivery capabilities and data retention.

167. New subsection 317T(12) requires that a technical capability notice specify an ‘applicable costs negotiator’ for the notice. This is the person who will settle the basis of

compliance for the notice and the terms and conditions of any requirements in the notice under new subsections 317ZK(3) and 317ZK(4).

168. By virtue of new subsection 317T(13), a person may be specified under new subsection 317T(12) by name or by position.

317TAA – Provision of advice to designated communications providers

169. New section 317TAA requires the Attorney-General to advise a designated service provider of their obligations to comply with a technical capability notice if they have been issued with a notice. The obligations to comply with a notice are provided in section 317ZA for carriers and carriage service providers, and section 317B for designated communications providers (other than carriers and carriage service providers). This provision ensures that providers understand their obligations in either 317ZA or 317ZB so far as they relate to the technical capability notice.

317TA – Duration of technical capability notice

170. A technical capability notice comes into force when given or when specified in the notice. Notices only remain in force until the expiry date specified in the notice or, in cases where no expiry date was specified, at the end of 180 days after issue.

317U – Compliance period etc.

171. New section 317U specifies that a technical capability notice may require that a thing required in a notice be done in a specified period of time, a specified manner, or in a way that meets one or more specified conditions.

317V - Decision-making criteria

172. New section 317V inserts a requirement that, before giving a technical capability notice, the Attorney-General must be satisfied that the requirements imposed by the notice are reasonable and proportionate, and compliance with the notice is practicable and technically feasible. This criterion is exercised in the same manner as decisions made by the Director-General of Security or the chief officer of an interception agency for issuing technical assistance notices under new section 317P.

173. The conditions of reasonableness, proportionality, practicability and technical feasibility will be harder to meet in the case of a technical capability notice. The simple fact that these notices require a provider to build something that goes beyond current business requirements will raise thresholds, particularly those of proportionality and reasonableness.

174. Satisfaction is a subjective state of mind of the administrative decision-maker. It is a precondition to the exercise of the power. To meet the requisite state of satisfaction the decision-maker must consider the reasonableness and proportionality of the requirements imposed by the notice and the practicability and technical feasibility of compliance with that notice. The decision-maker's satisfaction must be formed on a correct understanding of the law.[5] The decision-maker must not take into account a consideration which a court can

[5] *Minister for Immigration and Multicultural Affairs v Eshetu* (1999) 197 CLR 611 at 651-654.

determine in retrospect 'to be definitely extraneous to any objects the legislature could have had in view.'[6]

175. This means the Attorney-General must evaluate the individual circumstances of each notice. In deciding whether a notice is reasonable and proportionate, it is necessary for the Attorney-General to consider both the interests of the agency and the interests of the provider. This includes the objectives of the agency, the availability of other means to reach those objectives, the likely benefits to an investigation and the likely business impact on the provider. It is important that the provider is the most appropriate person to provide the assistance sought by the agency. For example, a notice given to a provider who, while able to assist, did not control the relevant data and was not in a position to help as adequately as a more directly related provider would not be proportionate. In that instance it would need to be clear that the controller of the data was unable or unwilling to assist.

176. The Attorney-General must also consider wider public interests, such as any impact on privacy, cyber security and innocent third parties. In deciding whether compliance with the notice is practicable and technically feasible, the Attorney-General must consider the systems utilised by a provider and provider expertise. To be satisfied, the Attorney-General would need to consider material information given to Government by the provider. It is expected that the relevant agency would be engaged in a dialogue with the provider prior to making a request to the Attorney-General. The Attorney-General may also make inquiries with other persons who have relevant experience and technical knowledge.

177. The same principles that govern the nature of satisfaction in 317L apply in this section.

317W – Consultation about a proposal to give a technical capability notice

178. The Attorney-General must undertake a consultation process before a provider is subject to a legal obligation to comply with a technical capability notice. New subsection 317W(1) imposes a requirement on the Attorney-General to give a provider a written notice setting out a proposal to give the notice and inviting that person to make a submission on the proposal.

179. Paragraph 317W(1)(b) provides that the Attorney-General is only required to take into account representations made within the specified 28 day timeframe. This qualification will ensure that notices can be issued and implemented in a timely manner.

180. New subsection 317W(1) does not restrict the Attorney-General from consulting with other persons. This could include other Ministers with an interest, such as the Minister for Communications and the Arts.

181. New subsection 317W(2) requires the consultation period to run at least 28 days. However, the provision does not prevent the Attorney-General from allowing a provider more than 28 days in which to make representations. In practice, it is expected that consultation periods will be agreed between Government and industry, with discussions about the feasibility of a notice occurring prior to issue.

[6] *Water Conservation and Irrigation Commission (NSW) v Browning* (1947) 74 CLR 492 at 505.

182. New subsection 317W(3) states that the consultation period may be shortened if the Attorney-General is satisfied of any of the following conditions:

a. the notice should be given as a matter of urgency, or

b. compliance with the consultation period is impracticable, or

c. the provider waives the consultation requirement.

183. For example, a shorter timeframe may be required where a capability can be built to prevent imminent harm to the public or where there is a serious risk that material evidence will be lost without the assistance of a provider.

184. New subsection 317(4) and (5) state that where a provider waives the consultation period it may be orally or in writing. However if the waiver is oral, a written record must be provided within 48 hours by the provider.

185. New subsection 317W(7) allows the Attorney-General and the provider to jointly appoint a technical expert for the purpose of gauging whether a proposed technical capability notice would contravene section 317ZG. Given the likely sensitivity surrounding the capabilities of both the designated communication provider and the requesting agency it is important that the technical expert is mutually agreed.

186. A report of the assessment must be provided to both the Attorney-General and the provider within the time limit specified in the consultation notice. An assessment conducted by a jointly appointed person provides greater certainty in situations where there are concerns that the proposal in a technical capability request may require the provider to implement or build a systemic weakness or systemic vulnerability. Under new subsection 317(11), information in relation to carrying out the assessment, and that contained in the report, is taken to be information that falls within the definition of **technical capability notice information**.

187. New subsection 317(8) ensures the Attorney-General and the provider only appoints a person that has the necessary knowledge to determine if the proposed technical capability notice would contravene section 317ZG. This ensures that only those persons with the technical knowledge and expertise are appointed to make this judgement given the likely complexity of the notice. Systemic weaknesses or vulnerabilities may be difficult to determine and third party technical expert may assist.

188. New subsection 317W(9) places the financial obligations with the provider for engaging one or more persons under 317W(7). Under new subsection 317W(10) the Attorney-General, on behalf of the Commonwealth, may consider reimbursing the whole or part of the amount of any remuneration paid by a designated communications provider to a person or persons appointed under subsection 317(7).

317X – Variation of technical capability notices

189. New section 317X allows the Attorney-General to vary a technical capability notice that has been given to a provider. Variations must be made in writing.

190. The requirements of a notice may be ongoing in nature and the capabilities built under them of lasting utility. Accordingly, it may be necessary to vary the requirements of a notice to respond to developments in a provider's services, the roll-out of new technology or a change in agency practices. Variation of a notice may also be required in response to shifts in operational priorities and emergency circumstances. Variation may be more efficient and effective than the issuing of a new technical capability notice.

191. Consistent with the process for variation of technical assistance notices in new subsection 317Q(8), new subsections 317X(2) and 317X(3) require that the variation must be connected to the eligible activities of a provider and covered by the requirements in new subsection 317T(2).

192. The variation may be in relation to a capability required to be built under a technical capability notice or in relation to assistance (where the provider has an existing capability) required to be given under a technical capability notice.

193. New subsection 317X(3) provides that where the variation is in relation to a capability required to be built under a technical capability notice, the thing specified in the varied notice must be a listed act or thing in section 317E (other than the act of thing covered by paragraph 317E(1)(a)) or a thing the Minister determines by legislative instrument. Paragraph 317E(1)(a) lists removing electronic protection. This means that a varied technical capability notice cannot require the building of a decryption capability.

194. Where the variation is in relation to assistance the provider has the capability to provide, the thing specified in the varied notice may include, but is not limited to, a listed act or thing in section 317E.

195. The Attorney-General must not vary a notice unless satisfied that the requirements imposed are reasonable and proportionate and compliance with the varied notice is practicable and technically feasible.

196. New subsection 317X(4) ensures that variations are made consistent with the same decision-making requirements that governed the original decision.

317Y – Consultation about a proposal to vary a technical capability notice

197. New section 317Y requires the Attorney-General consult with a provider before varying a technical capability notice. The consultation process is consistent with the process under 317W for the issuing of a notice. The Attorney-General must give a provider a written notice setting out a proposal to vary the notice and inviting that person to make a submission on the proposal.

198. The consultation period must run for at least 28 days. However, the Attorney-General may allow a provider more than 28 days to make representations.

199. The consultation period may be shortened if the Attorney-General is satisfied that the notice should be varied as a matter of urgency, compliance is impracticable or the provider waives the requirement.

317Z – Revocation of technical capability notices

200. New subsection 317Z(1) allows the Attorney-General to revoke a technical capability notice. Revocation must be in writing to the person to whom the notice was given.

201. New subsection 317Z(2) requires the Attorney-General to revoke a technical capability notice if satisfied that the requirements imposed by the notice are not reasonable and proportionate or that compliance with the warrant is not practicable and technically feasible. Changing business requirements, developments in technology or shifts in the operational priorities of agencies may render the acts or things specified in a notice inconsistent with these statutory requirements. The revocation provision establishes an avenue to discontinue notices that have become obsolete or excessively burdensome.

317ZAA – Whether requirements imposed by a technical capability notice are reasonable and proportionate

202. New section 317ZAA requires that, in determining whether a technical capability notice or varied technical capability notice is reasonable and proportionate, the Attorney-General must have regard to the following matters:

a. the interests of national security;

b. the interests of law enforcement;

c. the legitimate interests of the designated communications provider to whom the notice relates;

d. the objectives of the notice;

e. the availability of other means to achieve the objectives of the notice;

f. the legitimate expectations of the Australian community relating to privacy and cybersecurity; and

g. any other matters (if any) that the Attorney-General considers to be relevant.

Division 5 – Compliance and enforcement

203. Division 5 establishes a framework for compliance with the requirements of a technical assistance notice or technical capability notice and sets out the enforcement remedies available to pursue compliance.

204. Separate regimes apply to carriers and carriage service providers and other categories of designated communications providers. Carriers and carriage service providers will continue to be regulated under the Telecommunications Act. Other enforcement options will apply to companies and people who are not subject to the regulatory measures in the Act.

205. The Communications Access Co-ordinator, a statutory body within the Department of Home Affairs, serves an administrative function in new Part 15 and is the relevant applicant for the enforcement remedies available in this Division. The Co-ordinator may apply for civil penalties, enforceable undertakings and injunctions in the Federal Court or the Federal

Circuit Court of Australia where a provider has not been compliant with their obligations under a technical assistance notice or technical capability notice.

206. The remedies available have been calculated to achieve the primary aim of deterrence and are proportionate to the seriousness of contravention. Non-compliance with technical assistance notices and technical capability notices may have significant consequences for law enforcement and national security.

207. Technical assistance notices and technical capability notices are not subject to merits review. As opposed to judicial review, which ensures that decisions were made within the legal limits of the relevant power, merits review aims to ensure the 'correct' decision is made. The merits review body remakes the decision. Excluding merits review in relation to decisions made under new Part 15 of the Act is consistent with other decisions made for national security and law enforcement purposes – for example those made under the IS Act, ASIO Act, IGIS Act and the TIA Act. Decisions of a law enforcement nature were identified by the Administrative Review Council in its publication *What decisions should be subject to merits review?* as being unsuitable for merits review.

208. Security and law enforcement agencies may require a technical assistance notice to facilitate lawful access to electronic evidence for an investigation that is underway and evolving. It is imperative that a technical assistance notice can be issued and used quickly to ensure fast and efficient access to the necessary information. It would not be appropriate for a decision to issue a technical assistance notice to be subject to merits review as review could adversely impact the speed and outcomes of the investigation.

209. Decisions by the Attorney-General to issue a technical capability notice are particularly unsuitable for merits review. A technical capability notice may be issued to assist urgent national security and serious criminal investigations, but may also be issued to require agencies to build a standing capability to assist agencies in an ongoing fashion. In these latter circumstances, the Attorney-General's decision will involve complex policy questions that have affects beyond the provider issued with a warrant. The decisions will involve balancing different interests, using a range of information sources available to the Attorney-General by virtue of his or her portfolio responsibilities. As the Administrative Review Council recognises, where complex or political considerations exist, it is appropriate for the decision to rest with the executive arm of government.

210. These new powers have in-built safeguards that are designed to ensure that the scope of the powers does not go beyond what is reasonable and necessary to assist agencies in the exercise of their functions and powers under law.

317ZA Compliance with notices and warrants—carriers and carriage service providers

211. New section 317ZA requires carriers and carriage service providers served with a technical assistance notice or technical capability notice to comply with that notice to the extent that they are capable of doing so.

212. For the purposes of new subsection 317ZA(1), capable means that carriers and carriage service providers must have the resources, or the means to acquire the resources, for complying with a notice. This ensures that if extenuating circumstances prevent a provider from meeting the full requirements of a notice, then they are only obliged to meet the requirements to the extent possible.

213. Contravention of new section 317ZA attracts the pecuniary penalties in Part 31 of the Act (see the note to new section 317ZA). This means carriers and carriage service providers face the same penalties for not complying with technical assistance notices and technical capability notices, as other civil penalty provisions in the Telecommunications Act. For example, non-compliance with a notice carries the same civil penalties as a breach of a carrier licence held by the carrier. This is also consistent with penalties associated with a carrier's failure to comply with their duty to give reasonably necessary assistance under section 313 of the Telecommunications Act.

214. Civil action may be taken to recover those penalties. The penalties in Part 31 are proportionate to the offence and appropriate to achieve the primary aim of deterrence. The maximum penalty for corporate entities is set to account for significant resources of the corporate entities that will likely be subject to the powers in new Part 15.

215. New subsection 317ZA(2) prohibits persons from doing things to bring about the contravention of subsection (1). These include, aiding, abetting, inducing or conspiring to affect a contravention of a carrier's or carriage service provider's obligation to comply with a technical assistance notice or technical capability notice.

317ZB Compliance with notices and warrants—designated communications provider (other than a carrier or carriage service provider)

216. New section 317ZB requires designated communications providers (other than carriers and carriage service providers) served with a technical assistance notice or technical capability notice to comply with that notice to the extent that they are capable of doing so. Capable means that providers must have the resources, or the means to acquire the resources, for complying with a notice.

217. Under new subsection 317ZB(1), the civil penalty for non-compliance by body corporates is 47,619 penalty units and the civil penalty for non-compliance by persons who are not body-corporates is 238 penalty units. These penalties are equivalent with the penalties applicable to carriers and carriage service providers for breach of a carrier licence in Part 31 of the Telecommunications Act.

218. Consistent with the rationale for enforcement elsewhere in the Telecommunications Act, the penalty units in new section 317ZB are calculated to achieve deterrence and are set proportionally to the limits of seriousness for contravention. The broad range of entities that may be subject to requirements in new Part 15 requires a higher maximum penalty. The supply of communications services and devices can be a highly profitable enterprise and many providers that fall within the scope of items 4 – 15 in the table in new section 317C have significant financial reserves. Lower maximum penalties would be unlikely to achieve deterrence.

219. The penalty amounts also reflect the significant loss that may result from non-compliance with a notice. Failure to act in good faith with any requirements may jeopardise ongoing criminal investigations, result in the destruction of material evidence or, in extreme cases, expose the Australian public to serious and imminent harm.

220. New subsection 317ZB(3) expressly excludes subsection 82(5) of the Regulatory Powers Act from applying to a contravention of new subsection 317ZB(1). Subsection 82(5) provides that the pecuniary penalty for breach by a body corporate must not be more than 5

times the pecuniary penalty specified for breach by an individual. Exclusion of subsection 82(5) of the Regulatory Powers Act to the operation of 317ZB(1) is necessary to account for the broad array of entities that may be subject to technical assistance notices and technical capability notices. In order to achieve the primary aim of deterrence from corporate entities of significant wealth, it is appropriate to set significant maximum penalties. However, a penalty one fifth of the maximum which corporate entities are subject to paying may be too high for individuals.

221. New subsection 317ZB(4) provides that section 564 and section 572B do not apply to a contravention of new subsection 317ZB(1). Section 564 provides that a court may grant injunctions in relation to contraventions of the Act and section 572B provides that a person may give an enforceable undertaking about compliance with the Act. These remedies have been provided for in new sections 317ZC, 317ZD and 317ZE which implements Parts 4, 6 and 7 of the Regulatory Powers Act (civil penalty, enforceable undertaking and injunctions provisions, respectively).

222. New subsection 317ZB(5) provides a defence to a civil penalty proceeding for not meeting the obligations under subsection 317ZB(1), if in complying with the requirements of a technical assistances notice or technical capability notice, the provider contravenes a law of a foreign country. The provider bears the onus of proof for this provision to apply. This provision ensures that a provider is not prosecuted for non-compliance with a notice if, at the time the notice was given, the provider would have breached foreign laws in order to comply with the notice.

317ZC – Civil penalty provision

223. New section 317ZC provides that new section 317ZB is enforceable under Part 4 of the Regulatory Powers Act. This Part allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

224. New subsection 317ZC(2) provides that the Communications Access Co-ordinator, a statutory body within the Department of Home Affairs, is an authorised applicant in relation to new section 317ZB. New subsection 317ZC(3) provides that the Federal Court and the Federal Circuit Court of Australia are relevant courts in relation to new section 317ZB. An authorised application may apply to a relevant court for an order that a person who is alleged to have contravened a civil penalty provision, pay the Commonwealth a pecuniary penalty.

225. New subsection 317ZC(4) makes clear that Part 4 of the Regulatory Powers Act extends to every external Territory and acts, omissions, matters and things outside Australia. The extension of jurisdictions reflects the scope of providers that may be issued a technical assistance notice or technical capability notice.

317ZD – Enforceable undertakings

226. New section 317ZD provides that new section 317ZB is enforceable under Part 6 of the Regulatory Powers Act. This Part enables an authorised person to accept written undertakings committing a person to particular action (or inaction) in order to prevent or respond to a breach of an enforceable provision. Undertakings are enforceable in their own right and they may be entered into instead of, or in addition to, the authorised person taking other disciplinary action.

227. New subsection 317ZD(2) provides that the Communications Access Co-ordinator is an authorised person in relation to new section 317ZB. This includes accepting undertakings and applying to court for an order directing a provider to comply with an undertaking. New subsection 317ZD(3) stipulates that the Federal Court and the Federal Circuit Court of Australia are relevant courts in relation to section 317ZB.

228. New subsection 317ZD(4) extends the territorial application of Part 6 of the Regulatory Powers Act as it relates to section 317ZB to every external Territory and acts, omissions, matters and things outside Australia. The extension of jurisdictions reflects the scope of providers that may be issued a technical assistance notice or technical capability notice.

317E – Injunctions

229. New section 317ZE incorporates injunctions under Part 7 of the Regulatory Powers Act as a remedy for enforcement of new section 317ZB. Injunctions may be used to restrain a person from contravening a provision enforceable under this Part, or to compel compliance with such a provision.

230. New subsection 317ZE(2) provides that the Communications Access Co-ordinator is an authorised person in relation to section 317P. New subsection 317ZE(3) provides that the Federal Court and the Federal Circuit Court of Australia are relevant courts in relation to section 317ZB.

231. The Communications Access Co-ordinator may make an application to the Federal Court or Federal Circuit Court of Australia for an injunction under this section.

232. New subsection 317ZE(4) extends the territorial application of Part 7 of the Regulatory Powers Act as it relates to section 317ZB to every external Territory and acts, omissions, matters and things outside Australia. The extension of jurisdictions reflects the scope of providers that may be issued a technical assistance notice or technical capability notice.

Division 6 - Unauthorised disclosure of information

233. Division 6 provides an offence for disclosing information relating to a technical assistance notice, technical capability notice and technical assistance request. The purpose of the provisions is to protect both designated communications providers, and law enforcement and security agencies. It is designed to restrict the disclosure of commercially sensitive information, as well as highly sensitive information pertaining to investigations and agency capabilities more broadly. Disclosure of such information could damage providers and compromise law enforcement and national security outcomes.

234. Exceptions to the unauthorised disclosure offence enable the ready exchange of information where necessary for the administration of Part 15, or where relevant for the performance of the functions and powers of law enforcement, security and intelligence agencies.

317ZF - Unauthorised disclosure of information

235. New subsection 317ZF(1) creates an offence where any of the following persons disclose technical assistance notice information, technical capability notice information or technical assistance request information (or information obtained in accordance with a request or notice):

i. a designated communications provider
ii. an employee of a designated communications provider
iii. a contracted service provider of a designated communications provider
iv. an employee of a contracted service provider of a designated communications provider
v. an entrusted ASIO person
vi. an entrusted ASIS person
vii. an entrusted ASD person
viii. an officer of an interception agency
ix. an officer or employee of the Commonwealth, a State or a Territory
x. a person appointed under subsection 317W(7), or
xi. an arbitrator appointed under new section 317ZK, where parties disagree on the terms and conditions relating to a requirement in a technical assistance notice or technical capability notice.

236. New paragraph 317ZF(1)(d) requires a connection between the identity of the person, the activities of the person and the way in which the relevant information came to that person's knowledge or into that person's possession. The paragraph provides that if the person is or was:

i. a designated communications provider, the person must have received the relevant information in connection with his or her capacity as such a provider
ii. an employee of a designated communications provider, the person must have received the relevant information because he or she was employed by the provider in connection with its business as such a provider
iii. a contracted service provider of a designated communications provider, the person must have received the relevant information in connection with his or her business as such a contracted service provider
iv. an employee of a contracted service provider of a designated communications provider, the person must have received the relevant information because he or she was employed by the contractor in connection with its business as such a contracted service provider
v. an entrusted ASIO person, the person must have received the relevant information in his or her capacity as such an entrusted person
vi. an entrusted ASIS person, the person must have received the relevant information in his or her capacity as such an entrusted person
vii. an entrusted ASD person, the person must have received the relevant information in his or her capacity as such an entrusted person
viii. an officer of an interception enforcement agency, the person must have received the relevant information in his or her capacity as such an officer
ix. an officer or employee of the Commonwealth, a State or a Territory, the person must have received the relevant information in his or her capacity as such an officer or employee

x. an arbitrator appointed under section 317ZK, the person must have received the relevant information in his or her capacity as such an arbitrator.

237. This connection ensures that a person who received information innocently or without reference to their functions under new Part 15 is not liable for an offence under new subsection 317ZF(1). The prohibition on disclosure applies in relation to a person's activities as an employee or contractor of a provider or in a person's capacity as a government official. This is consistent with the responsibilities of persons who hold these positions.

238. The offence in new subsection 317ZF(1) does not include an express requirement of harm, and therefore, the prosecution is not required to prove harm beyond reasonable doubt. There is a high risk that the release of sensitive information contrary to this subsection will cause significant harm to essential public interests, including national security and protection of public safety. Therefore, it is assumed that disclosure is inherently harmful.

239. The maximum penalty for this offence is 5 years imprisonment. This penalty is appropriate to achieve the primary aim of deterrence and proportionate to the seriousness of contravention. The information protected by this provision is highly sensitive, and the consequences of the commission of the offence may be dangerous or damaging to national security. The maximum penalty of 5 years is equivalent with the penalties for unauthorised disclosure of information by entrusted persons in section 35P of the ASIO Act. It is also consistent with the Australian Law Reform Commission 2009 Report on Secrecy Law and Open Government in Australia which provides guidelines in considering the proportionality of penalties associated with the breach of secrecy provisions.

240. New subsection 317ZF(3) outlines the circumstances in which disclosures are permitted. A person may disclose information:

a. in connection with the administration or execution of this Part
b. for the purposes of any legal proceedings arising out of or otherwise related to this Part or of any report of any such proceedings
c. in accordance with any requirement imposed by law of the Commonwealth, a State or a Territory
d. in connection with the performance of functions, or the exercise of powers by ASIO, ASIS, ASD, or an interception agency
e. for the purpose of obtaining legal advice in relation to this Part
f. to an IGIS official for the purpose of IGIS exercising powers or performing functions or duties under the IGIS Act.
g. if the person himself or herself is an IGIS official, in connection with his or her exercise of powers or performance of functions under the IGIS Act.

241. Under new paragraph 317ZF(3)(a) a person is permitted, for example, to disclose information for the purposes of giving, or varying, a technical assistance request, technical assistance notice or technical capability notice. A person is also permitted to disclose information for the purpose of complying with a technical assistance request, technical assistance notice or technical capability notice.

242. For the purposes of new paragraph 317ZF(3)(b) legal proceedings include civil proceedings a provider is party to and are relevant to claims of civil immunity under 317G or 317ZJ. This paragraph also includes legal proceedings relevant to the telecommunications and computer offences under Part 10.6 and Part 10.7 of the Criminal Code.

243. In addition, a disclosure that is authorised under new subsections 317ZF(5), 317ZF(6), 317ZF(7), 317ZF(8), 317ZF(9) or 317ZF(10) or 317ZF(11) is permitted.

244. The note following new subsection 317ZF(2) indicates that where a person is charged in relation to a contravention of section 317ZF, the defendant bears an evidential burden to demonstrate that the disclosure was lawful due to the application of an exception. This is consistent with evidential principles in the Criminal Code.

245. The exceptions in new subsection 317ZF(3) allow for the smooth administration of the Part and for the efficient exchange of information within law enforcement, security and intelligence agencies that seek or require assistance from providers.

246. New subsection 317ZF(4) makes clear that this Part also includes any other provision of this Act, so far as that other provision relates to this Part, and Regulatory Powers Act so far as that Act relates to this Part.

247. New subsections 317ZF(6)-(11) make clear that the Director-General of Security, the Communications Access Coordinator and the chief officer of an interception agency may share information with one another without committing an offence. The chief officer of an interception agency may also share information with ASIS and ASD. However, the sharing of information permitted under new subsections (6)-(11) must be for purposes relating to those persons' performance of functions, or their exercise of powers. These subsections are consistent with the practical assistance agencies frequently provide to one another and existing information-sharing arrangements. It is important for the effective execution of their national security and law enforcement functions. The efficient exchange of information is particularly necessary where shared capabilities are developed under a technical capability notice.

248. New subsection 317ZF(12) provides that before disclosing any information to another agency allowed under subsections (6)-(10), the Director-General of Security, the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Signals Directorate, or the chief officer of an interception agency must notify the Communications Access-Co-ordinator. This is designed to assist the Communications Access-Co-ordinator in its administration of the powers in the Act.

249. New subsection 317ZF(13) provides that providers may also disclose statistical information about the total number of notices or requests issued to them in a period of at least 6 months. This allows providers to publish aggregates of notices or requests received from Australia in transparency reports. It does not allow for the publication of statistics by issuer or agency and must relate to total numbers only. Any statistic that identifies the issuing agency would be in breach of the unauthorised disclosure offence.

250. All disclosures not prohibited by new section 317ZF are authorised by law for the purposes of the Privacy Act 1988.

317ZFA – Powers of a court

251. New section 317ZFA provides powers to the court to ensure information in relation to a technical assistance notice information, a technical capability notice information and a technical assistance request is protected appropriately without adversely impacting the interests of the issuer, the communications provider or the public. This provision will

complement existing protections in the *National Security Information Act 2004*, the *Surveillance Devices Act 2004* and the *Telecommunications (Interception and Access) Act 1979.*

252. Subsection 317ZFA(1) allows the court to make such orders as the court considers appropriate in relation to the disclosure, protection, storage, handling or destruction of technical assistance notice information, technical capability notice information and technical assistance request information if the court is satisfied it is in the interests of the public interest. Subsection 317ZFA(1)(a)-(b) limits these orders to proceedings under, or arising out of:

a. Part 15 of the *Telecommunications Act 1997*; or

b. any other provision of this Act, so far as that other provision relates to Part 15 *Telecommunications Act 1997*; or

c. the *Regulatory Powers (Standard Provisions) Act 2014*, so far as that Act relates to Part 15 *Telecommunications Act 1997*.

253. Subsection 317ZFA(2) clarifies that the powers vested with the court in subsection 317ZFA(1) are in addition to any other powers of the court.

254. Section 317ZFA is modelled on subsection 19(1A) of the *National Security Information Act 2004.*

Division 7—Limitations

255. Division 7 sets out limitations on technical assistance notices and technical capability notices.

317ZG – Designated communications provider must not be required to implement or build systemic weakness or systemic vulnerability etc.

256. New section 317ZG ensures that providers cannot be required to systemically weaken their systems of electronic protection under a technical assistance notice or technical capability notice. The limitation is designed to protect the fundamental security of software and devices. It ensures that the products Australians enjoy and rely on cannot be made vulnerable to interference by malicious actors.

257. Under new paragraph 317ZG(1)(a), a technical assistance notice or technical capability notice has no effect to the extent it requires a designated communications provider to build or implement a systemic weakness, or a systemic vulnerability, into a form of electronic protection. Electronic protection includes forms of encryption or passcode authentication, such as rate limits on a device.

258. A technical assistance notice or technical capability notice may, notwithstanding new paragraph 317ZG(1)(a), require a provider to enable access to a particular service, particular device or particular item of software, which would not systemically weaken these products across the market. For example, if an agency were undertaking an investigation into an act of terrorism and a provider was capable of removing encryption from the device of a terrorism suspect without weakening other devices in the market then the provider could be compelled

under a technical assistance notice to provide help to the agency by removing the electronic protection. The mere fact that a capability to selectively assist agencies with access to a target device exists will not necessarily mean that a systemic weakness has been built. The nature and scope of any weakness and vulnerability will turn on the circumstances in question and the degree to which malicious actors are able to exploit the changes required,

259. Under new paragraph 317ZG(1)(b), a technical assistance notice or technical capability notice has no effect to the extent it prevents a provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection. This means that a technical assistance notice or technical capability notice cannot be used to prohibit a provider from fixing flaws across their services or devices.

260. Likewise, a notice or warrant may require a provider to facilitate access to information prior to or after a method of electronic protection is employed, as this does not weaken the electronic protection itself. A requirement to disclose an existing vulnerability is also not prohibited by 317ZG(1)(a).

261. New subsection 317ZG(2) clarifies that a provider cannot be required to build a new decryption capability into a form of electronic protection.

262. New subsection 317ZG(3) clarifies that a provider cannot be required to do anything that would render systemic methods of authentication or encryption less effective.

263. New subsection 317ZG(4) clarifies that subsections (2) and (3) are enacted for the avoidance of doubt and do not change the ordinary meaning of the terms 'systemic weakness' or 'systemic vulnerability'.

264. New subsection 317ZG(5) ensures that a technical assistance notice or technical capability notice is invalid to the extent to which it would cause a systemic weakness or vulnerability in a form of electronic protection.

317ZH – General limits on technical assistance notices and technical capability notices

265. New subsection 317ZH(1) provides that a technical assistance notice or technical capability notice has no effect to the extent it requires a designated communications provider to do an act or thing which would require a warrant or authorisation under the TIA Act, the SD Act, the Crimes Act, the ASIO Act, or the IS Act. This ensures that a technical assistance notice or technical capability notice cannot be used as an alternative to a warrant or authorisation under any of those acts. For example, a technical assistance notice or technical capability notice cannot require a provider to intercept communications; an interception warrant under the TIA Act would need to be sought. However, a technical assistance notice under new section 317L or a technical capability notice under new section 317T may require a provider to assist with the access of information or communications that have been lawfully intercepted.

266. New subsection 317ZH(2) provides that, for the purpose of the limitation in subsection 317ZH(1), you assume that each law applies inside and outside Australia and that any reference in Part 13 to carriage service provider includes a reference to a designated communications provider. This ensures that technical assistance notices and technical capability notices cannot be used to require offshore providers to do things, which would require a warrant or authorisation if they were a carrier or carriage service provider. For

example, a technical assistance notice cannot compel the production of telecommunications data, as this would require an authorisation under the TIA Act if the provider were a carrier.

267. New subsection 317ZH(3) provides that a technical assistance notice or technical capability notice has no effect to the extent it requires a designated communications provider to use a surveillance device or access data held in a computer where a State or Territory law requires a warrant or authorisation for that use or access. This ensures that a technical assistance notice or technical capability notice cannot be used as an alternative to a warrant or authorisation under State or Territory law.

268. New subsection 317ZH(4) makes clear that, notwithstanding subsections (1) and (3), a technical assistance notice or technical capability notice may require a designated communications provider to assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or Territory or give effect to a warrant or authorisation under a law of the Commonwealth.

269. New subsection 317ZH(5) makes clear that, notwithstanding subsections (1) and (3) a technical capability notice may require a provider to develop a capability if the capability would assistant in giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory or give effect to a warrant or authorisation under a law of the Commonwealth.

Division 8—General provisions

270. Division 8 establishes the framework for civil immunity for things done in compliance with a notice. The Division also sets out the terms and conditions on which assistance is provided, the financial arrangements that govern this assistance and the procedure for service of notices.

317ZJ - Immunity

271. New subsection 317ZJ(1) provides designated communications providers immunity from civil liability for, or in relation to, any act or thing done in compliance, or in good faith in purported compliance, with a technical assistance notice or technical capability notice. It is full immunity for civil actions brought under Commonwealth law.

272. ‘Purported compliance’ means that providers are not liable to an action or other proceeding in the exceptional circumstances where some elements of a technical assistance notice or technical capability notice are deemed invalid. A provider acts in good faith if the provider acts with honesty according to the standards of a reasonable person.

273. New subsection 317ZG(2) means that immunity will not extend to an act or thing done by a provider unless the act or thing is connected to their eligible activities in section 317C. Providers cannot act outside their activities and receive immunity for those actions.

274. New subsection 317ZJ(3) extends this immunity to officers, employees and agents of providers who perform an act or thing in connection with the provider’s actions to comply, or purportedly comply in good faith, with a technical assistance notice or technical capability notice.

317ZK – Terms and conditions on which help is to be given etc.

275. New section 317ZK applies if a person is required to provide help under new technical assistance notice or technical capability notice issued in accordance with new sections 317L and 317T, respectively. It sets out the terms of compliance and the framework for arbitration where parties fail to reach agreement on the conditions of compliance.

276. New subsection 317ZK(3) states that, generally, compliance with requirements is on a no profit or loss basis. New paragraph 317ZK(3)(b) notes that the provider is not expected to bear the reasonable costs of complying with a requirement. The 'reasonable costs' of compliance may be different from the actual costs of meeting the requirements in a notice. For example, if a provider's expenditure is higher than necessary to satisfy their obligations under new Part 15, they are entitled to recover costs equivalent to the expenditure that would have been reasonable to satisfy requirements.

277. However, different cost arrangements may be agreed by the provider and the *applicable costs negotiator* (defined in new subsection 317ZK(16)). In the case of a technical assistance notice, this is the Director-General of Security or the chief officer of an interception agency and in the case of a technical capability notice, it is a person specified by the notice in accordance with new subsection 317T(12) and 317T(13).

278. Commercial terms may be appropriate where agencies require a provider to develop a large bespoke capability that would ordinarily be the subject of a significant procurement. The availability of commercial terms will give the agency the flexibility to enter into an arrangement containing both financial incentives and risk-management measures to secure satisfactory and timely performance.

279. The process for determining the terms and conditions of compliance are set out in new subsections 317ZK(4) - (6). Generally, the terms and conditions will be set by agreement between the provider and the applicable costs negotiator. Where these parties fail to reach an agreement, an arbitrator approved by both parties will determine the terms and conditions of compliance. In the event that both parties cannot agree on the appointment of an arbitrator, an arbitrator is appointed by the ACMA (if the provider is a carrier or carriage service provider) or by the Attorney-General (for other classes of designated communications provider).

280. Under new subsection 317ZK(8) and subsection 317ZK(11) the relevant Minister can specify one or more persons, or a class of persons, to be suitable for appointment as an arbitrator. New subsection 317ZK(9) makes clear that an instrument under subsection 317ZK(8) is not a legislative instrument. It is administrative rather than legislative in character, as the instrument does not determine or alter the law. Before making these specifications, the relevant Minister must consult with the Attorney-General. If an arbitration is conducted by an arbitrator appointed by the ACMA, then the cost of arbitration must be shared equally between the parties. Where the arbitrator is appointed by the Attorney-General, the relevant Minister may make provisions relating to the conduct of arbitration, including provisions relating to the costs of arbitration.

281. In limited circumstances it may be appropriate that the costs of complying with a technical assistance notice or technical capability notice are not recoverable. New subsections 317ZK(1) and (2) create a public interest exception where the Director-General of Security or the chief officer of an interception agency is satisfied it would be contrary to the public interest for a notice to be settled in accordance with the terms and conditions in subsections

317ZK(3) and (4). The Attorney-General may invoke an identical public interest exception for managing compliance with a technical capability notice. In some circumstances it will not be appropriate to compensate a provider subject to a notice, for example where it has been issued to remediate a risk to law enforcement or security interests that has been recklessly or wilfully caused by a provider.

282. The threshold for exercising this public interest exemption is high. New subsection 317ZK(2) requires that The Director-General of Security, the chief officer of an interception agency or the Attorney-General, as the case may be, must be satisfied that waiving the established compliance processes is in the public interest, and turn their mind to a range of commercial, law-enforcement and security considerations, including:

a. the interests of law enforcement

b. the interests of national security

c. the objects of the Telecommunications Act

d. the extent to which compliance with the requirement will imposed a regulatory burden on the provider

e. the reasons for the giving of the technical assistance notice or technical capability notice, and

f. such other matters that the decision-maker considers relevant.

283. New subsection 317ZK(15) provides that section 317ZK has no effect to the extent (if any) to which its operation would result in an acquisition of property otherwise than on just term.

284. An applicable costs negotiator for the purposes of section 317ZK is defined in new subsection 317ZK(16). For requirements under a technical assistance notice, the Director-General or the chief officer of an interception agency is the applicable costs negotiator as the case may be. For requirements issued under a technical capability notice, the applicable costs negotiator is the person specified in the notice in accordance with new subsection 317T(11).

317ZL - Service of notices etc

285. New section 317ZL is a deeming provision setting out when a summons, process, technical assistance notice or technical capability notice is taken to have been served on, or given to, a designated communications provider or to a body corporate incorporated outside Australia.

286. New subsection 317ZL(2) provides that service of a required summons, process, notice or warrant on a designated communications provider has taken place if it is left at, or sent by pre-paid post to, an address given by the provider.

287. New subsection 317ZL(3) provides that service of a required summons, process, notice or warrant on a designated communications provider has taken place if it is sent to an electronic address given by the provider.

288. New subsection 317ZL(4) provides that if a summons, process, notice or warrant is required to be served on, or given to, a body corporate that is incorporated outside Australia, does not have a registered or principal office in Australia, and has an agent in Australia, the summons, process, notice or warrant can be served on, or given to the agent of the body corporate in Australia.

289. New subsection 317ZL(5) provides that if a summons, process, notice or warrant is required to be served on, or given to, a body corporate that is incorporated outside Australia, does not have a registered or principal office in Australia, and carries on business or conducts activities at an address in Australia, the summons, process, notice or warrant can be served on, or given to the body corporate if it is left at, or sent by pre-paid post to, that address.

290. New subsection 317ZL(6) clarifies that subsections (2), (3), (4) and (5) have effect in addition to section 28A of the Acts Interpretation Act 1901 and sections 587 and 588 of the Telecommunications Act, which deal with the service of documents.

317ZM – Interception agency—chief officer and officer

291. The table in new section 317ZM defines a chief officer of an interception agency and officer of an interception agency for the purposes of new Part 15. The name of the interception agency is provided in column 1, the definition of chief officer of the interception agency is provided in column 2 and the definition of officer of the interception agency is provided in column 3.

292. Item 1 of the table lists the Australian Federal Police. Chief officer means the Commissioner in section 6 of the *Australian Federal Police Act 1979*. Officer means a member of the Australian Federal Police under section 40B of that Act or a special member under section 40E of that Act.

293. Item 2 of the table lists the Australian Commission for Law Enforcement Integrity. Chief officer means the Integrity Commissioner appointed under section 175 of the *Law Enforcement Integrity Commissioner Act 2006*. Officer means either the Integrity Commissioner or a staff member of ACLEI within the meaning of subsection 11(1) of that Act.

294. Item 3 of the table lists the Australian Crime Commission. Chief officer means the Chief Executive Officer of the Australian Crime Commission appointed under section 37 of the *Australian Crime Commission Act 2002*. Officer means either the Chief Executive Officer of the Australian Crime Commission, or an examiner appointed under subsection 46B(1) of that Act, or a member of the staff of the ACC within the meaning of section 4 of that Act.

295. Item 4 of the table lists the Police Force of a State or the Northern Territory. Chief officer means the Commissioner of Police, however designated, of that State or Territory. Officer means an officer of that Police Force.

296. Item 5 of the table lists the Independent Commission Against Corruption of New South Wales. Chief officer means the Chief Commissioner appointed under section 104 of the *Independent Commission Against Corruption Act 1988* (NSW). Officer means an officer of the Commission within the meaning of section 3 of that Act but it does not include a person engaged under section 104B of that Act to provide the Commission with services, information or advice.

297. Item 6 of the table lists the New South Wales Crime Commission. Chief officer means the Commissioner appointed under section 8 of the *Crime Commission Act 2012* (NSW). Officer means an officer of the Commission within the meaning of section 72 of that Act but it does not include a person engaged by the Commission as a consultant under subsection 74(2) of that Act.

298. Item 7 of the table lists the Law Enforcement Conduct Commission of New South Wales. Chief officer means the Chief Commissioner appointed under section 18 of the *Law Enforcement Conduct Commission Act 2016* (NSW). Officer means either the Chief Commissioner, or the Commissioner for Integrity appointed under section 18 of that Act, or an Assistant Commissioner appointed under section 20 of that Act, or a member of the staff of the Commission within the meaning of section 21 of that Act.

299. Item 8 of the table lists the Independent Broad-based Anti-corruption Commission of Victoria. Chief officer means the Commissioner appointed under section 20 of the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic.). Officer means a sworn IBAC Officer within the meaning of section 3 of that Act.

300. Item 9 of the table lists the Crime and Corruption Commission of Queensland. Chief officer means the chairperson within the meaning of the *Crime and Corruption Act 2001* (Qld). Officer means a commission officer as defined by paragraph (a) of the definition of commission officer in the Dictionary to that Act. Officer does not mean a person engaged under section 256 of that Act to provide the Commission with services, information or advice.

301. Item 10 of the table lists the Independent Commissioner Against Corruption (SA). Chief officer means the Commissioner appointed under section 8 of the *Independent Commissioner Against Corruption Act 2012* (SA). Officer means either: the Commissioner, or the Deputy Commissioner appointed under section 9 of that Act, or a member of the staff of the Independent Commissioner Against Corruption (SA) within the meaning of section 12 of that Act.

302. Item 11 of the table lists the Corruption and Crime Commission (WA). Chief officer means the Commissioner appointed under section 9 of the *Corruption, Crime and Misconduct Act 2003* (WA). Officer means an officer of the Commission within the meaning of section 3 of that Act. Officer does not mean a person engaged under section 182 of that Act to provide the Commission with services, information or advice.

317ZN - Delegation by Director-General of Security

303. New section 317ZN allows the Director-General of Security to delegate any of his or her functions or powers under Divisions 2, 3 or 6 to a senior position-holder in the ASIO Act. Under section 4 of that Act, a senior position-holder means an ASIO employee or an ASIO affiliate who holds, or is acting in, a position that is: equivalent to or higher than a position occupied by an SES employee; or known as Coordinator.

304. The purpose of this delegation power is to enable persons with appropriate seniority and expertise to perform functions or powers. In doing so, it allows for processes to be streamlined in order to assist ASIO to discharge its statutory functions. In accordance with usual administrative law practices, the delegation must be in writing and specify to whom the

function or power is delegated. The delegate must also comply with any written directions of the Director-General of Security.

305. Consistent with paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901*, the powers of the Director-General of Security that may be delegated under new section 317ZN do not include that power to delegate. This means that sub-delegation of powers and functions of the Director-General of Security is prohibited. This ensures that only persons of sufficient seniority may issue technical assistance requests and technical assistance notices and disclose information in accordance with new section 317ZF.

317ZP - Delegation by Director-General of the Australian Secret Intelligence Service

306. New section 317ZP allows the Director-General of the ASIS to delegate any of his or her functions or powers under new Divisions 2 and 6 to a staff member of ASIS who holds, or is acting in, a position in ASIS that is equivalent to, or higher than, a position occupied by an SES employee.

307. This delegation supports the efficient exercise of the powers under new Part 15 and ensures these powers are limited to persons of appropriate seniority and expertise.

308. Consistent with paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901*, the powers of the Director-General of the Australian Secret Intelligence Service that may be delegated under new section 317ZP do not include that power to delegate. This means that sub-delegation of powers and functions of the Director-General of the Australian Secret Intelligence Service is prohibited. This ensures that only persons of sufficient seniority may issue technical assistance requests and disclose information in accordance with new section 317ZF.

317ZQ - Delegation by Director of the Australian Signals Directorate

309. New section 317ZQ allows the Director of ASD to delegate any of his or her functions or powers under new Divisions 2 and 6 to a staff member of the ASD who holds, or is acting in, a position in the ASD that is equivalent to, or higher than, a position occupied by an SES employee.

310. This delegation supports the efficient exercise of the powers under new Part 15 and ensures these powers are limited to persons of appropriate seniority and expertise.

311. Consistent with paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901*, the powers of the Director of the Australian Signals Directorate that may be delegated under new section 317ZQ do not include that power to delegate. This means that sub-delegation of powers and functions of the Director of the Australian Signals Directorate is prohibited. This ensures that only persons of sufficient seniority may issue technical assistance requests and disclose information in accordance with new section 317ZF.

312. A delegate must comply with any written directions of the chief executive.

317ZR - Delegation by the chief officer of an interception agency

313. New section 317ZR allows the chief officer of an interception agency, listed in Column 1 of the item, to delegate any of his or her functions or powers under new Divisions

2, 3 or 6 to persons mentioned in Column 2 of the item. This delegation supports the efficient exercise of the powers under new Part 15 and ensures these powers are limited to persons of appropriate seniority and expertise.

314. Consistent with paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901*, the powers of the chief officer of an interception agency that may be delegated under new section 317ZR do not include that power to delegate. This means that sub-delegation of powers and functions of the chief officer of an interception agency is prohibited. This ensures that only persons of sufficient seniority may issue technical assistance requests and technical assistance notices and disclose information in accordance with new section 317ZF.

315. Item 1 of the table provides that the chief officer of the AFP may delegate his or her functions or powers to either a Deputy Commissioner in section 6 of the *Australian Federal Police Act 1979* or a senior executive AFP employee within the meaning of section 25 of that Act.

316. Item 2 of the table provides that the chief officer of the Australian Commission for Law Enforcement Integrity may delegate his or her functions or powers to either an Assistant Integrity Commissioner appointed under section 185 of the *Law Enforcement Integrity Commissioner Act 2006* or a staff member of ACLEI within the meaning of subsection 11(1) of that Act who is an SES employee or acting SES employee.

317. Item 3 of the table provides that the chief officer of the Australian Crime Commission may delegate his or her functions or powers to a member of the staff of the ACC within the meaning of section 4 of the *Australian Crime Commission Act 2002* who is an SES employee or acting SES employee.

318. Item 4 of the table provides that the chief officer of a Police Force of a State or the Northern Territory may delegate his or her functions or powers to either an Assistant Commissioner of the Police Force or a person holding equivalent rank, or a Superintendent of the Police Force or a person holding equivalent rank.

319. Item 5 of the table provides that the chief officer of the Independent Commission Against Corruption of New South Wales may delegate his or her functions or powers to either a Commissioner appointed under section 5 of the *Independent Commission Against Corruption Act 1988* (NSW), or an Assistant Commissioner appointed under section 6A of that Act, or an officer of the Commission within the meaning of section 3 of that Act (other than a person engaged under section 104B of that Act) who is at executive level.

320. Item 6 of the table provides that the chief officer of the New South Wales Crime Commission may delegate his or her functions or powers to an officer of the Commission within the meaning of section 72 of the *Crime Commission Act 2012* (NSW) (other than a person engaged under subsection 74(2) of that Act) who is at executive level.

321. Item 7 of the table provides that the chief officer of the Law Enforcement Conduct Commission of New South Wales may delegate his or her functions or powers to either the Commissioner for Integrity appointed under section 18 of the *Law Enforcement Conduct Commission Act 2016* (NSW), or an Assistant Commissioner appointed under section 20 of that Act, or a member of the staff of the Commission within the meaning of section 21 of that Act who is at executive level.

322. Item 8 of the table provides that the chief officer of the Independent Broad-based Anti-Corruption Commission of Victoria may delegate his or her functions or powers to either a Deputy Commissioner of the Commission appointed under section 23 of the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic.), the Chief Executive Officer of the Commission appointed under section 33 of that Act, or a sworn IBAC officer within the meaning of section 3 of that Act who is at executive level.

323. Item 9 of the table provides that the chief officer of the Crime and Corruption Commission of Queensland may delegate his or her functions to a senior executive officer within the meaning of paragraphs 245(3)(b) and 245(3)(a) of the *Crime and Corruption Act 2001* (Qld).

324. Item 10 of the table provides that the chief officer of the Independent Commissioner Against Corruption (SA) may delegate his or her functions to either the Deputy Commissioner within the meaning of the *Independent Commissioner Against Corruption Act 2012* (SA) or a member of staff of the Independent Commissioner Against Corruption within the meaning of that Act who is at executive level.

325. New subsection 317ZR(2) provides that a delegate must comply with any written directions of the chief executive.

326. New subsection 317ZR(3) clarifies the term executive level, which appears in the table in relation to an interception agency of New South Wales. Subsection 317ZR(3) provides that for the purposes of new section 317ZR, a person is at executive level if the person occupies an office or position at an equivalent level of a Public Service senior executive within the meaning of the *Government Sector Employment Act 2013* (NSW).

327. New subsection 317ZR(4) clarifies the term executive level, which appears in the table in relation to an interception agency of Victoria. Subsection (4) provides that for the purposes of new section 317ZR, a person is at executive level if the person occupies an office or position at an equivalent level of an executive within the meaning of the *Public Administration Act 2004* (VIC).

328. New subsection 317ZR(5) clarifies the term executive level, which appears in the table in relation to an interception agency of South Australia. Subsection (5) provides that for the purposes of new section 317ZR, a person is at executive level if the person occupies an office or position at an equivalent level of an executive employee within the meaning of the *Public Sector Act 2009* (SA).

317ZS – Annual reports

329. New subsection 317ZS introduces annual reporting requirements connected to the exercise of powers in new Part 15. The Minister must cause a written report to be prepared that sets out the number of technical assistance requests and technical assistance notices given under section 317G and 317L during the financial year by chief officers of interception agencies. This report must set out the number of technical capability notices given under section 317T that were issued to build capabilities used by interception agencies.

330. Reports under new subsection 317ZS are included in the annual report under Chapter 4 of the TIA Act which discloses information on the use of telecommunications data by law enforcement agencies.

317ZT – Alternative constitutional basis

331. New section 317ZT provides an alternative constitutional basis for Part 15. It ensures that, in cases where the constitutional support for making a request, or issuing a notice or warrant, to a provider is not made out under other heads of power in the Constitution, the scope of 317E should be read down as if the corporation's power was the sole basis for constitutional authority.

Part 2 – Amendments contingent on the commencement of the Federal Circuit and Family Court of Australia Act 2018

332. References to the 'Federal Circuit Court of Australia' 317ZC(3), 317ZD(3) and 317ZE(3) are to be omitted and substituted with 'Federal Circuit and Family Court of Australia' upon enactment of the Federal Circuit and Family Court of Australia (Consequential Amendments and Transitional Provisions) Bill 2018, Federal Circuit and Family Court of Australia Bill 2018

Schedule 2 – Computer access warrants

Part 1 – Amendments

Australian Security Intelligence Organisation Act 1979

Item 1 – Section 4

333. This item provides that 'intercept a communication passing over a telecommunications system' is given the same meaning in the ASIO Act as under the TIA Act.

334. The TIA Act provides that a communication which is listened to, or recorded by any means, without the knowledge of the person making it, between being sent or transmitted by the person sending it and becoming accessible to the intended recipient, is intercepted passing over a telecommunications system (see sections 5F, 5G, 5H and 6).

335. This ensures the terminology used across both Acts in relation to the interception of telecommunications is consistent.

336. The definition facilitates new provisions that allow for interception to occur where necessary to execute a computer access warrant. New paragraph 25A(4)(ba) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing things specified in the computer access warrant.

337. The definition also facilitates new provisions that allow for interception to occur where necessary to execute an identified person warrant in relation to accessing data held in computers. New paragraph 27E(2)(ea) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything authorised under an identified person warrant in relation to accessing data held in computers.

Item 2 – Subsection 24(4) (definition of *relevant device recovery provision)*

338. This item includes new subsection 25A(8) in the list of provisions defined as 'relevant device recovery provisions' for the purposes of section 24.

339. Section 24 states that the authority conferred by a relevant warrant or relevant device recovery provision may be exercised on behalf of ASIO by the Director-General or persons he or she appoints in writing.

340. This means the authority conferred by subsection 25A(8), which permits the concealment of activities undertaken under a computer access warrant following the expiry of

that warrant, is to be exercised only by the Director-General, or a person or class of persons approved by the Director-General in writing.

341. This item provides a safeguard against the arbitrary exercise of the range of activities permitted by the new subsection by requiring the person or class of persons exercising the authority to be approved by the Director-General personally.

Item 3 – Subsection 24(4) (definition of *relevant device recovery provision)*

342. This item includes subsection 27A(3C) and subsection 27E(6) in the list of provisions defined as 'relevant device recovery provisions' for the purposes of section 24.

343. This requires the authority conferred by these subsections—which permit the temporary removal of computers or other things for the purposes of concealing access, and the concealment of access to a computer or thing under an identified person warrant, respectively—to be exercised only by the Director-General, or a person or class of persons approved by the Director-General in writing.

344. As with item 2, this item provides a safeguard against the arbitrary exercise of the range of activities permitted by these new subsections by requiring the person or class of persons exercising these powers to be approved by the Director-General personally.

Item 4 – Paragraph 25A(4)(ab)

345. This item replaces paragraph 25A(4)(ab) with a new paragraph which reformats the same content. The requirements of the paragraph are now presented as a numbered list. The intention of the change is to simplify the presentation of the content, not to change the content or meaning of the paragraph.

Item 5 – After paragraph 25A(4)(ab)

346. This item inserts a new paragraph to permit the removal of a computer or other thing from premises, for the purposes of doing anything specified in a computer access warrant, before returning the computer or other thing to the premises.

347. ASIO does not currently have authority to temporarily remove a computer from a premises for the purposes of executing a computer access warrant. However, ASIO does have authority to temporarily remove objects from premises for the installation or maintenance of a surveillance device (see paragraph 26B(4)(b)).

348. The ability to remove computers from premises is important in situations where ASIO may require specialist equipment, which cannot be brought onto the premises in a covert fashion, in order to access the computer.

349. The deprivation of property is an intrusive measure. The item limits the degree of intrusion by confining the authority to a specific purpose and requiring the return of the computer or thing once the purpose is achieved. The removal of a computer or other thing is only permitted for the purposes of doing anything specified in the computer access warrant before the computer or other thing must be returned to the premises.

350. The authority is only available where the Attorney-General considers it appropriate in the circumstances, further safeguarding against its arbitrary exercise, and oversight is conducted by the IGIS to ensure the power is exercised lawfully, with propriety and with respect for human rights.

Item 6 – After paragraph 25A(4)(b)

351. This item inserts a new paragraph to permit the interception of a communication passing over a telecommunication system, if the interception is for the purposes of doing anything specified in the computer access warrant.

352. It is almost always necessary for ASIO to undertake limited interception for the purposes of executing a computer access warrant. Currently, ASIO is required to obtain a computer access warrant under section 25A, 27A or 27E of the ASIO Act to gain access to a device, and a telecommunications interception warrant under section 9 or 9A of the TIA Act to intercept communications.

353. The threshold requirements for issuing computer access warrants and telecommunication interception warrants currently differ.

354. In some circumstances, ASIO can obtain a computer access warrant, but cannot obtain a telecommunications interception warrant. This reduces the likelihood of a successful execution of the validly issued computer access warrant. It is undesirable for ASIO's ability to execute a computer access warrant to be dependent on its ability to obtain a separate telecommunications interception warrant. Ordinarily, warrants authorise a person to undertake all activities normally required to give effect to the warrant, independently of any other warrant or authorisation.

355. The current arrangements also cause administrative inefficiency by requiring ASIO to prepare two warrant applications, addressing different legal standards, for the purpose of executing a single computer access warrant. The process requires the Attorney-General to consider each application separately and in accordance with each separate criterion.

356. The amendments also include provisions tightly constraining the purposes for which ASIO may use information intercepted under this provision, consistent with Parliament's intention for interception warrants to be subject to higher statutory thresholds than computer access warrants. These are discussed at items 124 – 131A.

Item 7 – At the end of section 25A

357. This item inserts a new subsection 25A(8) relating to concealment of access under computer access warrants.

358. Currently, ASIO does not have authority to retrieve or delete remnants of its computer access activities, or to conceal the activities it has undertaken pursuant to a computer access warrant, following the expiry of the warrant. By contrast, ASIO does have authority to undertake a range of activities to recover surveillance devices following the expiry of the relevant surveillance device warrant under subsection 26B(5) of the ASIO Act.

359. ASIO cannot always reliably predict whether, or when, it will be able to safely retrieve its devices without compromising a covert security intelligence operation. For

example, a person may unexpectedly relocate their computer or device prior to the expiry of the warrant, precluding ASIO from taking the necessary steps to conceal the fact that it had accessed the device under warrant until the computer or device is available to be access again.

360. Once the warrant has expired ASIO may not be able to obtain a further computer access warrant to undertake retrieval and concealment activities, as retrieving and concealing would (by definition) not necessarily meet the statutory threshold of 'substantially assisting the collection of intelligence'.

361. The inserted provisions will provide ASIO with the ability to retrieve devices following the expiry of a computer access warrant in order to undo any additions, deletions or alterations made in the target computer, which it was not previously able to do.

362. The item provides that ASIO may perform these concealment activities 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.

363. The period of time provided to perform these concealment activities recognises that, operationally, it is sometimes impossible for ASIO to complete this process within 28 days of a warrant expiring. The requirement that the concealment activities be performed 'at the earliest time after than 28-day period at which it is reasonably practicable to do so' acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.

Item 8 – After subsection 27A(3B)

364. This item inserts a new subsection relating to concealment of access under computer access warrants for foreign intelligence. It is ASIO's function to obtain and communicate foreign intelligence within Australia under paragraph 17(1)(e).

365. This provision permits ASIO to do specified things, and things 'reasonably incidental' to a specified thing, to conceal the fact that anything has been done in connection with a foreign intelligence warrant that authorises ASIO to do acts or things referred to under a computer access warrant.

366. The item is consistent with the approach taken in subsection 27A(3A) for the recovery of surveillance devices installed or used under a foreign intelligence warrant.

Item 9 – Paragraph 27E(2)(d)

367. This item replaces paragraph 27E(2)(d) with a new paragraph which reformats the same content. The requirements of the paragraph are now presented as a numbered list. The intention of the change is to simplify the presentation of the content, not to change the content or meaning of the paragraph.

Item 10 – After paragraph 27E(2)(d)

368. This item inserts provisions allowing for the removal of a computer or thing from the premises for the purposes of an identified person warrant. Specifically, it allows ASIO to

remove and return a computer or other thing from premises for the purposes of doing anything authorised under an identified person warrant in relation to the computer.

369. Identified person warrants may be issued where the Attorney-General is satisfied that a person is engaged, or reasonably suspected of being engaged or likely to engage in, activities prejudicial to security, and that issuing a warrant in relation to that person will, or is likely to, substantially assist the collection of intelligence relevant to security. This is a higher threshold than for standard computer access warrants under section 25A.

370. Identified person warrants can give conditional approval for ASIO to access records or other things in or on premises, access data held in computers, use one or more kinds of surveillance devices, access postal articles that are in the course of post, and access articles that are being delivered by a delivery service provider.

371. However, conditional approval does not, of itself, authorise ASIO to do things under an identified person warrant. Things can only be done under the warrant if ASIO is subsequently authorised to do those things under sections 27D - 27H. Relevantly, section 27E applies where ASIO has conditional approval to access data held in computers under an identified person warrant.

372. This item will ensure that things that may be authorised under an identified person warrant in relation to data held in computers mirrors those things that may be authorised under a computer access warrant once amended (see paragraph 25A(4)(ac)). It will ensure consistency between the functionality of these two warrants where either is issued for the purpose of computer access.

Item 11 – After paragraph 27E(2)(e)

373. This item inserts provisions allowing a communication passing over a telecommunications system to be intercepted if the interception is for the purposes of doing anything authorised under an identified person warrant in relation to accessing data held in computers.

374. As with item 10, this item will ensure that things that may be authorised under an identified person warrant in relation to data held in computers mirror those things that may be authorised under a computer access warrant once amended (see paragraph 25A(4)(ba)). This will ensure consistency between the functionality of these two warrants where either is issued for the purpose of computer access.

Item 12 – At the end of section 27E

375. This item inserts a new subsection relating to concealment of access under an identified person warrant in relation to accessing data held in computers. It mirrors the new subsection relating to concealment of access under a computer access warrant (see subsection 25A(8)).

376. This item permits ASIO to do anything reasonably necessary to conceal the fact that anything has been done under the warrant, and provides ASIO with the ability to retrieve devices following the expiry of a warrant in order to undo any additions, deletions or alterations made in the target computer.

377. ASIO may perform these concealment activities 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.

378. The period of time provided to perform these concealment activities recognises advice from ASIO that, operationally, it is sometimes impossible to complete this process within 28 days of a warrant expiring. The requirement that the concealment activities be performed 'at the earliest time after the 28-day period at which it is reasonably practicable to do so' acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.

Item 13 – Subsection 33(1)

379. This item repeals subsection 33(1) which provides that computer access warrants (section 25A), foreign intelligence warrants (section 27A) and authorisations under identified person warrants to access data held in computers (section 27E) do not authorise the interception of a communication passing over a telecommunications system.

380. This provision is inconsistent with the amendments discussed above which introduce measures allowing for the interception of a communication passing over a telecommunications system in certain limited circumstances under each of these warrants.

Item 14 – Paragraph 34(2)(b)

381. This item imposes additional reporting requirements on the Director-General in relation to concealment of access and temporary removal under computer access warrants (subsections 25A(8) and 27A(3C) respectively). The report which the Director-General is required to furnish to the Attorney-General in respect of these warrants must include details of anything which materially interfered with, interrupted or obstructed the lawful use by other persons of a computer or other electronic equipment or data storage device.

382. This supplements the requirement for all warrants issued under Division 2 of the ASIO Act to be reported on in relation to the extent to which the action taken under each warrant assisted ASIO in carrying out its functions.

383. This item recognises that the authority for ASIO to conceal access and temporarily remove computers and other things under a computer access warrant is an intrusive measure, which requires proportionate safeguards. ASIO computer access warrants should not ordinarily interfere with a person's use of a computer. Requiring ASIO to bring material interferences to the Attorney-General's attention will ensure that the Attorney-General is aware of issues and can consider the implications when deciding whether to issue future warrants.

Item 15 – Paragraph 34(2)(b)

384. This item imposes additional reporting requirements on the Director-General in relation to concealment of access under an identified person warrant in relation to data held in computers (subsection 27E(6)).

385. This supplements the requirement for all warrants issued under Division 2 of the ASIO Act to be reported on in relation to the extent to which the action taken under each warrant assisted ASIO in carrying out its functions.

386. As with item 14, this item recognises that the authority for ASIO to conceal access to data held in computers under an identified person warrant is an intrusive measure, which requires proportionate safeguards. ASIO identified person warrants should not ordinarily interfere with a person's use of a computer. Requiring ASIO to bring material interferences to the Attorney-General's attention will ensure that the Attorney-General is aware of issues and can consider the implications when deciding whether to issue future warrants.

Item 16 – At the end of section 34

387. This item clarifies that anything done to conceal access to a computer or other thing under a computer access warrant or an identified person warrant is to be taken, for the purposes of section 34, as having been done under that warrant.

388. This will ensure that concealment activities are captured by section 34 and will be subject to reporting requirements.

Item 17 – Subsection 34AA(5) (definition of *relevant authorising provision)*

389. This item includes subsection 25A(8) as a 'relevant authorising provision' for the purposes of evidentiary certificates in relation to warrants.

390. This allows the Director-General to issue a written certificate setting out facts in relation to ASIO's concealment activities under a computer access warrant, which provides prima facie evidence of the matters stated in it for the purposes of proceedings.

Item 18 – Subsection 34AA(5) (definition of *relevant authorising provision)*

391. This item includes subsections 27A(3C) and 27E(6) as 'relevant authorising provisions' for the purposes of evidentiary certificates in relation to warrants.

392. As with item 17, this allows the Director-General to issue a written certificate setting out facts in relation to the temporary removal of computers or other things under a computer access warrant, and the concealment of access under an identified person warrant in relation to data held in computers, respectively.

Mutual Assistance in Criminal Matters Act 1987

Item 25 – Subsection 3(1) (definition of *protected information*)

393. This item includes new paragraph 44(1)(aa) of the SD Act within the definition of protected information for the purposes of the MACMA. This means that any information (other than general computer access intercept information) obtained from access to data under either the new computer access warrant or emergency authorisation for access to data held in a computer is protected information.

394. The amendment extends the current definition of protected information which refers to information obtained from the use of a surveillance device or tracking device under warrant or authorisation (see paragraphs 44(1)(a), (b) and (c) of the SD Act).

395. This ensures that where information is obtained in response to a computer access warrant for a domestic investigation, the Attorney-General may authorise the provision of that information to a foreign country in response to a mutual assistance request, subject to existing restrictions under section 13A of the MACMA

Item 26 – After Part IIIBA

396. This item inserts new Part IIIBBA into the MACMA.

397. New Part IIIBBA will allow foreign authorities to make a request to the Attorney-General to authorise an eligible law enforcement officer to apply for a computer access warrant for the purposes of obtaining evidence to assist in a foreign investigation or investigative proceeding.

398. Investigations and prosecutions frequently involve criminal use of the internet and cross border storage of information. Australia's mutual assistance framework is critical in enabling Australian and foreign authorities access to information necessary to conduct and undertake criminal proceedings, amongst other things.

399. These amendments do not allow a foreign country's authorities to exercise computer access powers within Australia. Rather, when authorised by the Attorney-General, it allows for Australian law enforcement to undertake these activities on their behalf under the authority of an appropriate computer access warrant.

400. The Attorney-General in exercising his or her discretion on authorising the use of this power for a foreign country will be subject to specific restrictions, including:

a. that the investigation or investigative proceeding relates to a criminal matter involving an offence against the law of a foreign country punishable by a maximum penalty of imprisonment for 3 years or more, imprisonment for life or the death penalty (note under section 8 of the MACMA a request for assistance must be refused if it relates to an offence in which the death penalty may be imposed unless 'special circumstances' exist – for example where the requesting country has provided an undertaking that the death penalty will not be carried out)

c. that the investigation or investigative proceeding at (a) has commenced in the requesting country

d. the requesting country specifically requests that the Attorney-General arrange for access to the data held on the target computer.

e. a computer must meet the definition of *target computer* which is restricted under the proposed section 15CC(2) of the MACMA where the definition of *computer* has the same meaning as the SD Act.

401. In addition to the above, section 15CC(1)(c) allows the Attorney-General in authorising the use of the power under the MACMA to require that a requesting country provide appropriate undertakings. This will ensure that the computer evidence provided as a result of the computer access warrant is only used for the authorised purpose for which it was obtained and consistent with conditions around the destruction of the document or thing containing the data.

402. Subparagraph 15CC(1)(c)(iii) further allows the Attorney-General to require undertakings on any other matter he or she considers appropriate. The requirement for undertakings from a requesting country serves to empower the Attorney-General to make any such requirements that may arise that would not be otherwise countenanced by limitations on the use of information such as paragraph 15CC(1)(a) or failsafe provisions contained within subparagraphs 15CC(1)(c)(i) and 15CC(1)(c)(ii). An example of an undertaking could include one that material provided not be used or disclosed publicly in the foreign court before a certain date to minimise any impact on related Australian investigations or proceedings.

403. The note provided in section 15CC requires that a warrant for the purposes of a section 15CC authorisation can only be obtained where the eligible law enforcement officer reasonably suspects that access to the data held in the target computer is necessary for the foreign investigation or proceeding. This is in line with section subsection 27A(4) of the SD Act.

404. Complementary facilitating provisions are located in subsection 6(1) of the SD Act and are discussed in notes of items 5 and 6 of this schedule.

Surveillance Devices Act 2004

Item 27 – Title

405. This item amends the long form title of the Act to 'An Act to set out the powers of Commonwealth law enforcement agencies with respect to surveillance devices and access to data held in computers, and for related purposes.'

406. This item does not alter the short title by which it may be cited.

Item 28 – After paragraph 3(a)

407. This item amends the purposes of the SD Act to reflect the new power in the Act for law enforcement agencies to access data held in computers. It adds as a purpose the establishment of procedures for law enforcement officers to obtain warrants and emergency authorisations for access to data held in computers, consistent with the position of surveillance devices warrants and authorisations. This relates to criminal investigations and the location and safe recovery of children to whom recovery orders relate.

Item 29 – After paragraph 3(aa)

408. This item amends the purposes of the SD Act to reflect the new power in the Act for law enforcement agencies to access data held in computers. It adds as a purpose the establishment of procedures for law enforcement officers to obtain warrants for access to data held in computers in control order cases, consistently with the position of surveillance

devices warrants and authorisations. This relates to protecting the public from a terrorist act, preventing the provision of support for or facilitation of a terrorist act, preventing the provision of support for or facilitation of hostile activity by a foreign country or determining whether a control order has been or is being complied with.

Item 30 – After paragraph 3(b)

409. This item amends the purposes of the SD Act to include restrictions on the use, communication and publication of information that is obtained through accessing data held in computers or that is otherwise connected with computer data access operations.

Item 31 – Paragraph 3(c)

410. This item amends the purposes of the SD Act to include imposing requirements for the secure storage and destruction of records, and the making of reports, in relation with computer data access operations.

Item 32 – Subsection 4(1)

411. This item amends subsection 4(1) to clarify that the SD Act is not intended to affect any other law of the Commonwealth, a State or any law of a self-governing Territory that prohibits or regulates computer access.

412. The item clarifies this relationship to other laws in respect of computer access, consistent with the position of surveillance devices.

Item 33 – After subsection 4(4)

413. This item inserts new subsection (4A) to clarify that a warrant or an emergency authorisation may be issued or given under the Act for access to data held in a computer, in relation to a relevant offence or a recovery order. This replicates the clarification in existing subsection 4(4) relating to warrants and emergency authorisations regarding surveillance devices.

Item 34 – After subsection 4(5)

414. This item inserts new subsection (5A) to clarify that a warrant may be issued or given under the Act for access to data held in a computer, in relation to a control order. This replicates the clarification in subsection 4(5) relating to control orders regarding surveillance devices.

Item 35 – Subsection 6(1)

415. This item inserts definitions of carrier and communication in transit.

416. Carrier means either a carrier or carriage service provider within the meanings of the Telecommunications Act.

417. The definition of communication in transit means a communication (within the meaning of the Telecommunications Act) passing over a telecommunications network (within the meaning of that Act). This definition is consistent with the definition in the ASIO Act.

418. These definitions are inserted to facilitate provisions that allow limited interception to occur where necessary to execute a computer access warrant. Paragraph 27E(2)(h) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything specified in the warrant in accordance with subsection 27E(2).

Item 36 - Subsection 6(1) (definition of *computer*)

419. This item repeals the definition of computer and replaces it with the definition of computer that is in section 22 of the ASIO Act.

420. The definition of computer within the ASIO Act is preferred for consistency between Acts in the statute book. This will also ensure consistency between powers conferred under those Acts.

421. The repealed definition defines computer as any electronic device for storing or processing information. The repeal of this definition is not to be read as the former provision not being correct. Rather, the former definition was limited. The new definition takes into account the increasing use of distributed and cloud-based services for processing and storing data, and the fact that data commonly passes through networks of computers. It is no longer realistic for law enforcement agencies to identify one particular computer on which relevant data is stored in the context of an investigation. Individuals commonly have multiple computers and access to a variety of networks. The intention of the provisions is to enable law enforcement agencies to access those networks under one computer access warrant rather than seeking a warrant for each device.

422. For the avoidance of doubt, mobile phones are intended to be captured by the definition of computer.

423. Communication devices for storing and processing information which would not colloquially be termed ‘computers’, but which use computers or computing technology as their functional basis, are still intended to be captured within the new definition. For example security systems, internet protocol cameras and digital video recorders may be computers for the purpose of facilitating computer access.

Item 37 – Subsection 6(1)

424. This item provides the definitions for terms that facilitate the operation of the computer data access provisions.

425. The definition of *computer access warrant* has the meaning given it by section 27C or subsection 35A(4) or (5). Section 27C allows an eligible Judge or nominated AAT member to issue a warrant, upon he or she being satisfied of the relevant conditions contained in section 27C(1), including that there are reasonable grounds for the suspicion that access to data will be necessary in the course of the investigation. Computer access warrant under subsections 35A(4) and (5) means a warrant issued by an eligible Judge or nominated AAT member after they have given an emergency authorisation.

426. The definition of *control order access warrant* is a computer access warrant issued in response to an application under subsection 27A(6). Under subsection 27A(6) a law enforcement officer may apply for the issue of a computer access warrant if a control order is

in force and he or she suspects that access to data held in a computer would be likely to substantially assist in either protecting the public from a terrorist act, preventing the provision of support for a terrorist act or a hostile activity, or determining whether the control order is being complied with.

427. The definition of *data* includes information in any form, as well as any program or a part of any program.

428. *Data held in a computer* includes data held in any removable data storage device for the time being held in a computer, and data held in a data storage device on a computer network of which the computer forms a part. This definition envisages both internal network storage, such as a back-up copy of data, and external storage, such as internet-based and cloud-based storage.

429. The definition of *data storage device* is consistent with the definition in section 4 of the ASIO Act and with the definition in the Criminal Code. The item defines data storage device to mean a thing containing, or designed to contain, data for use by a computer. This refers to things containing or designed to contain data for use by a computer. They do not need to be powered to qualify as a device. A CD, for example, is a data storage device. A data storage device becomes a constituent part of a computer once it is inserted into an optical drive for access to its data. A disc, compact disc, secure digital card (also known as an SD card), or any other thing that contains information that is made legible, accessible or usable by a computer are data storage devices. The definition is designed to cover future technological advancements.

Item 38 - Subsection 6(1) (definition of data surveillance device)

430. This item amends the definition of *data surveillance device* to accommodate for the new definition of computer in the SD Act (see item 36).

431. Data surveillance device means any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device.

Item 39 - Subsection 6(1)

432. This item inserts two new definitions into subsection 6(1).

433. General computer access intercept information is defined to have the same meaning as in the TIA Act. Item 120 inserts a definition of this new term into the TIA Act to mean information obtained under a general computer access warrant by intercepting a communication passing over a telecommunications system. This is distinct from a computer access warrant obtained by ASIO and distinct from computer data obtained under a computer access warrant.

434. Intercepting a communication passing over a telecommunications system has the meaning given to it by the TIA Act. The TIA Act defines interception of a communication passing over a telecommunications system as consisting of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication (see sections 5F, 5G. 5H and 6 of the TIA Act.)

435. Item 123 inserts the same definition into the section 4 of the ASIO Act.

Item 40 – Subsection 6(1) (definition of *mutual assistance application*)

436. This item replaces the definition of mutual assistance application to reflect the new power to apply for computer access warrants under the SD Act.

437. This schedule includes complementary amendments to the MACMA to enable mutual assistance applications to be made in regards to computer access warrants, consistent with the position of surveillance device warrants.

Item 41 – Subsection 6(1) (definition of *mutual assistance authorisation*)

438. This item amends the definition of mutual assistance authorisation to reflect the new power to apply for computer access warrants under the SD Act.

439. This Schedule includes complementary amendments to the MACMA to enable mutual assistance authorisations to be made in regards to computer access warrants, which enable mutual assistance applications.

Item 42 – Subsection 6(1) paragraph (db) of the definition of *relevant offence*

440. This item is a consequential amendment to capture new computer access warrants within the definition of relevant offences for integrity operations.

Item 43 – Subsection 6(1) (definition of *remote application*)

441. This item amends the definition of remote application in the SD Act to include reference to new section 27B of the Act. New section 27B allows for remote applications for computer data access warrants.

Item 44 – Subsection 6(1)

442. This item includes a definition of telecommunications facility within the SD Act. The term is defined to mean a facility within the meaning of the Telecommunications Act. New section 27E of the SD Act provides for a telecommunications facility to be used to obtain access to data under a computer access warrant.

Item 45 – Subsection 6(1) (definition of *unsworn application*)

443. This item includes references to provisions in relation to the new computer access warrants within the existing definition of unsworn application in the SD Act.

Item 46 – Subsection 6(1) (definition of *warrant*)

444. This item expands the existing definition of warrant to include the new computer access warrants introduced in the SD Act.

Item 47 – At the end of subsection 10(1)

445. This item expands the existing types of warrant that may be issued under Part 2 of the SD Act to include computer access warrants. This is consequential to the insertion of

Division 4 to Part 2 of the SD Act which establishes the framework for law enforcement agencies to obtain computer access warrants.

Item 48 – Subsection 10(2)

446. This item clarifies that a surveillance device warrant (or a retrieval warrant) may be issued in respect of more than one kind of surveillance device and more than one surveillance device of any kind.

447. This is a consequential amendment to ensure the expanded definition of warrant, including a computer access warrant, does not apply in relation to subsection 10(2).

Item 49 – At the end of Part 2

448. This item introduces Division 4 to Part 2 of the SD Act. Division 4 establishes the framework for law enforcement agencies to obtain computer access warrants. A computer access warrant enables officers to search electronic devices remotely and access content on those devices. These warrants are in addition to warrants for data surveillance devices, which enable the use of software to monitor inputs and outputs from certain devices.

27A - Application for a computer access warrant

449. Division 2 of the SD Act sets out the requirements and processes for obtaining a surveillance device warrant. Section 14 contains the provisions for applying for a surveillance device warrant. New section 27A replicates the structure of section 14, in providing for the application of computer access warrants in respect of offence investigations, recovery orders, mutual assistance investigations, integrity operations and control orders.

450. Section 14 contains a three part test that must be satisfied in order to apply for a surveillance device warrant. A law enforcement officer may apply for a surveillance device warrant if he or she suspects on reasonable grounds that one or more relevant offences have been or will be committed, that an investigation is or will be conducted, and that the use of a surveillance device is necessary in the course of that investigation for the purposes of enabling evidence to be obtained.

451. New section 27A preserves the threshold tests for making an application for a computer access warrant so that they are in line with the tests for an application for a surveillance device warrant in the SD Act. It will often be necessary for an agency to obtain both a surveillance device warrant and a computer access warrant in the course of one investigation.

452. A warrant can be sought in the context of an offence investigation if the law enforcement officer has reasonable grounds to suspect that a relevant offence is likely to be committed and investigated and access to data held in a computer is necessary for the purpose of enabling evidence to be obtained of either the commission of the offence or the identity or location of the offenders.

453. A law enforcement officer may apply for the issue of a computer access warrant if a recovery order is in force and he or she suspects on reasonable grounds that access to data held in the target computer may assist in the location and safe recovery of the child. A recovery order is either an order section 67U of the *Family Law Act 1975* or an order for a

warrant for the apprehension or detention of a child under regulations 15(1) or 25(4) of the *Family Law (Child Abduction Convention) Regulations 1986*.

454. A law enforcement officer may apply for a computer access warrant if he or she is authorised to do so under a mutual assistance authorisation and he or she suspects on reasonable grounds that access to data held in the target computer is necessary for the purpose of enabling evidence to be obtained of the commission of the commission of the offence to which the authorisation relates or the identity or location of the person suspected of committing the offence.

455. An integrity authority must be authorising an integrity operation in relation to an offence that is being committed by a staff member of a target agency, and the office must suspect on reasonable grounds that data held in the target computer will assist the obtaining of evidence relating to the integrity, location or identity of that person. Under the Act, an integrity authority is, an authority under Part IAB of the Crimes Act authorising either a controlled operation or an integrity testing operation.

456. This item enables computer access warrants to be sought in relation to control orders. Control orders are a protective mechanism under Division 104 of the Criminal Code that allows the Australian Federal Police to request that a court impose obligations, prohibitions and restrictions (controls) on a person for the purpose of protecting the public from a terrorist attack. Allowing computer access warrants to be sought in respect of control orders reflects the necessity of being able to monitor the online activity of people subject to control orders. Part of a control order may include, for example, a prohibition on viewing extremist material online.

457. In order to apply for computer access in relation to a control order, a control order must be in force, and the officer must suspect on reasonable grounds that access to data in the target computer will substantially assist in either protecting the public from a terrorist act, preventing support or facilitation of a terrorist act, preventing support or facilitation of engagement in hostile activity in a foreign country, or determining whether a control order is being complied with.

458. In each of subsections 27A(1), (3), (4), (5) and (6) the language ‘law enforcement officer, or another person on his or her behalf’ has been used to allow support staff engaged in the usual course of an investigation to assist or provide services. They are not specified in order to reflect that arrangements may differ between agencies.

459. Subsections 27A(9), (10), (11), (13) and (14) provide for applications for computer access warrants to be made before an affidavit is prepared or sworn under some circumstances. In those cases, the applicant must send a duly sworn affidavit to a Judge or AAT member no later than 72 hours after the making of the application. This enables an application to be made in circumstances where immediate access is necessary for the investigation.

460. Computer access warrants are sought for access to data held in the target computer. The definition of target computer is set out in new subsection 27A(15). The concept of the ‘target computer’ the same as in section 25A of the ASIO Act. The target computer may be either a particular computer, a computer on a particular premises, or a computer associated with, or used or likely to be used by a person. The computer does not need to be owned by

the suspect. For example, it might be a computer in the suspect's house that he or she uses but is not owned by the suspect.

461. The definition of 'target computer' should be read in conjunction with the new definition of 'computer' in the SD Act. While an application for a warrant must identify a target computer, this does not prevent access to data associated with the target computer on another computer (section 27E). The concept of the target computer is intended to ensure that if an individual has more than one relevant computer, only one warrant will be necessary. For example, there may be multiple computers on the premises and it may only be discovered upon entering that a particular computer is not connected to the anticipated computer system. With the variety of computers and electronic devices now commonly, it is highly probable that a person may store data on a number of computers (for example, a laptop, a phone and a tablet).

27B - Remote application

462. New section 27B permits the application for a computer access warrant to be made under section 27A by telephone, fax, email or by other means of communication where the law enforcement officer believes it is impracticable for the application to be made in person.

27C - Determining the application

463. New section 27C makes provisions for the conditions under which an eligible Judge or nominated AAT member may issue a computer access warrant. New section 27C is modelled on the current section 16. The issuing authority must be satisfied that there are reasonable grounds for the suspicion founding the application for the warrant.

464. In case of a warrant sought in relation to a relevant offence (paragraph 27C(1)(a)), the issuing authority may issue a computer access warrant if satisfied that there are reasonable grounds for the suspicion founding the application.

465. For a computer access warrant relating to a recovery order (section 27C(1)(b)), the issuing authority must be satisfied that there are reasonable grounds for the suspicion, and also that such a recovery order is in force. The same is the case for applications relating to mutual assistance authorisations (paragraph 27C(1)(c)).

466. If a warrant for computer access is sought in relation to an integrity operation, the issuing authority must be satisfied that the integrity authority for the operation is in effect and that there are reasonable grounds for the suspicions founding the application (paragraph 27C(1)(d)).

467. For a computer access warrant relating to a control order, in paragraph 27C(1)(e), (called control order access warrants), the Judge or AAT member must be satisfied that a control order is in force in relation to the person, and that access to data would likely substantially assist in protecting the public from a terrorist act, or preventing the support or facilitation of a terrorist act, or preventing the support of facilitation of hostile activity in a foreign country, or for determining whether a control order is being complied with.

468. For unsworn applications (paragraph 27C(1)(f)), the issuing authority must be satisfied that it was impracticable for an affidavit to have been sworn before the application was made. This allows for external scrutiny of judgments made by officers that an application

could not be made in person or that an affidavit could not be sworn in time. Similarly, in relation to applications made remotely, the eligible Judge or AAT member must also be satisfied that it was impracticable for the application to have been made in person.

469. Subsection 27C(2) sets out the considerations to which an issuing authority must have regard in determining whether a computer access warrant should be granted. The issuing authority must have regard to the extent to which the privacy of any person is likely to be affected and the existence of any alternative means of obtaining the evidence or information sought to be obtained. This applies to all matters for which a computer access warrant may be obtained.

470. For a warrant sought in relation to a relevant offence (paragraph 27C(2)(a)), the issuing authority must also have regard to the nature and gravity of the alleged offence, the likely evidentiary or intelligence value of any evidence that might be obtained, and any previous warrant sought.

471. For a warrant sought to assist in the locating and safe recovery of a child (paragraph 27C(2)(b)), the issuing authority must have regard to the circumstances which gave rise to the making of the order, and to any previous warrant sought.

472. For a warrant sought in relation to a mutual assistance authorisation (paragraph 27C(2)(f)), the issuing authority must also have regard to the nature and gravity of the alleged offence, and the likely evidentiary or intelligence value of any evidence that might be obtained but only to the extent that this is possible to determine from information obtained from the foreign country in question.

473. In determining whether a computer access warrant should be issued for an integrity operation (paragraph 27C(2)(e)), the issuing authority must have regard to the nature and gravity of the offence, and the likely evidentiary or intelligence value of any evidence or information sought to be obtained.

474. There are several mandatory considerations in determining an application relating to a control order (paragraphs 27C(2)(g) – (i) and (k)). They reflect the specifications that must be made in the application under subparagraph 27A(6)(b)(i)-(iv). The issuing authority must also consider the possibility that the person has engaged in a terrorist act, has provided support to or facilitated a terrorist act, has provided support for or facilitation of the engagement in a hostile activity in a foreign country, has contravened a control order, or might do any of these things.

27D - What must a computer access warrant contain?

475. Subsection 27D(1) sets out the information a computer access warrant is to contain. Every computer access warrant must contain the name of the applicant, the date the warrant is issued, either the computer or the premises to which the warrant relates, the period during which the warrant is in force and the name of the law enforcement officer primarily responsible for executing the warrant.

476. If the target computer is or includes a computer associated with, used by or likely to be used by a person, the warrant must also specify the person, whether by name or otherwise (subparagraph 27D(1)(b)(ix)).

477. Although the persons involved in the installation, maintenance or retrieval of a computer access device are not required to be named in the warrant itself, new subparagraph 49(2B)(b)(ii) requires that reports on computer access to the Minister must name each person involved in accessing data under the warrant.

478. In addition to the above requirements, warrants relating to one or more alleged relevant offences must specify those offences (subparagraph 27D(1)(b)(ii)).

479. Warrants relating to a recovery order must specify the date the order was made and the name of the child to whom the order relates (subparagraph 27D(1)(b)(iii)).

480. Warrants relating to a mutual assistance authorisation must specify the relevant offence or offences against the law of a foreign country (subparagraph 27D(1)(b)(iv)).

481. Warrants relating to an integrity operation must specify the integrity authority for the operation and each alleged relevant offence (subparagraph 27D(1)(b)(v)).

482. Subsection 27D(2) specifies that if a control order access warrant is issued, that warrant must also specify the name of the person subject to the control order, the date the control order was made, and whether the control order is an interim order or a confirmed control order.

483. Subsection 27D(3) provides that a computer access warrant may only be issued for a period of no more than 90 days, and no more than 21 days if it relates to an integrity operation.

484. Subsection 27D(4) provides that where a warrant authorises the use of a computer access device on a vehicle, the warrant need only specify a class of vehicle, thus minimising the risk of computer access being thwarted by frequent vehicle changes. The warrant may specify, for example, ‘a vehicle used by a specific person’, and this would be classified as a class of vehicle.

27E - What a computer access warrant authorises

485. A computer access warrant must authorise the doing of specified things in relation to the relevant target computer. The use of ‘must authorise’ differs from current section 18 of the SD Act which uses the term ‘may authorise’ because a surveillance device warrant is structured to be issued around a premises, a specified object or in respect of conversations. These location distinctions are not relevant to a computer access warrant which has as its object the computer itself, rather than an indistinct surveillance outcome which could require a device being placed in a variety of ways.

486. Subsection 27E(2) sets out the things that may be specified provided the eligible Judge or nominated AAT member considers it appropriate in the circumstances. As distinct from the previous paragraph, the word ‘may’ is used to clarify that all of the following particulars in paragraphs 27E(2)(a)-(i) are not required in every circumstance.

487. Under paragraph 27E(2)(a) the eligible Judge or AAT member may specify premises may be entered for the purposes of doing things mentioned in this subsection. Installation and retrieval of computer access devices may not always be performed remotely, and may involve some entry onto property. Paragraph 27E(2)(b) makes it clear that premises other than the

premises specified in a warrant (that is, third party premises) can be entered for the purpose of gaining access to or exiting the subject premises for the purposes of executing the computer access warrant. This may occur where there is no other way to gain access to the subject premises (for example, in an apartment complex where it is necessary to enter the premises through shared or common premises). It may also occur where, for operational reasons, the best means of entry might be through adjacent premises (for example, where entry through the main entrance may involve too great a risk to the safety of executing officers). The need to access third party premises may also arise in emergency and unforeseen circumstances (for example, where a person arrives at the subject premises unexpectedly during a search and it is necessary to exit through third party premises to avoid detection).

488. Under paragraph 27E(2)(c) the issuing authority may specify in the warrant that the warrant permits using the target computer, using a telecommunications facility operated or provided by the Commonwealth or a carrier, using any other electronic equipment or using a data storage device, for the purpose of obtaining access to data that is held in the target computer, in order to determine whether the relevant data is covered by the warrant. This is to ensure that data that is unknown or unknowable at the time the warrant has been issued can be discovered by using other means, in order to determine whether it is covered by the warrant. Data may need to be copied and analysed before its relevancy or irrelevancy is determined (paragraph 27E(2)(d)). Access to a secondary device, such as a USB, for example, may also be necessary in order to determine whether any data relevant to an investigation is held on the target computer. This would include access to any external storage devices, such as cloud-based data or any back-ups on other devices. Other electronic equipment might also include specialist communications equipment used within telecommunications transmittal devices.

489. Paragraph 27E(2)(c) makes clear by the words 'held in the target computer at any time while the warrant is in force' that computer access warrants authorise ongoing access to data held in the target computer over the life of the warrant. Data does not have to be stored on the target computer, but can be passing through it.

490. Paragraph 27E(2)(d) permits adding, copying, deleting or altering other data in the target computer if necessary to achieve the purpose mentioned in paragraph 27E(2)(c). Data may need to be copied and analysed before its relevancy or irrelevancy can be determined.

491. Paragraph 27E(2)(e) allows using any other computer or a communication in transit to access relevant data if it is reasonable in all the circumstances, having regard to other methods of obtaining access to the data. This ensures that law enforcement agencies can effectively use a third party computer or a communication in transit. Accessing a communication in transit means accessing any communication passing over a telecommunications network, between the target device and the service provider, as long as this access does not amount to interception. Whether access to a communication in transit is interception or not is dependent on what material could be or is gleaned from the action. Collecting contextual data which indicates a person's use of a computer would not constitute interception, whereas accessing the content of a person's communications would amount to interception. Permissible interception is provided for in paragraph 27E(2)(h).

492. The power to add, copy, delete or alter other data can only be used where necessary for the purpose of obtaining access to relevant data held in the target computer. This provision recognises that in some cases direct access to a target computer will be difficult or

even impossible. The use of third party computers and communications in transit to add, copy, delete or alter data in the computer or the communication in transit may facilitate that access.

493. In recognition of the privacy implications for third parties, in authorising the warrant the Judge or nominated AAT member must have regard to any other method of obtaining access to the relevant data which is likely to be as effective as accessing a third party's computer. This does not require all other methods of access to be exhausted, but rather allows the Judge or AAT member to take into account the circumstance before him or her and balance the impact on privacy with the risk of detection.

494. Paragraph 27E(2)(f) allows the removal of a computer or other thing from the premises for the purposes of executing the warrant, and returning the computer or other thing once it is no longer required. This includes the removal, for example of a USB key, a remote access token, or a password written on a piece of paper, from the premises, along with the computer.

495. Paragraph 27E(2)(g) allows the copying of any data which has been accessed if it either appears relevant for the purposes of determining whether the relevant data is covered by the warrant, or is covered by the warrant. Data that is subject to some form of electronic protection is taken to be relevant for the purposes of determining whether it is relevant data covered by the warrant (subsection 27E(3)). These provisions ensure that data either accessed on a computer remotely or accessed on a computer at the premises specified in the warrant can be copied onto another computer. This will be necessary in order for data to be analysed on a different computer located elsewhere or using different software. It will also be necessary for the collection of evidence.

496. Paragraph 27E(2)(h) permits intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything specified in the warrant in accordance with 27E(2).

497. Often it will be necessary for a law enforcement agency to intercept communications for the purpose of executing a computer access warrant. This subsection ensures that they will be able to do so, but only for those limited purposes of making computer access practicable or technically possible.

498. A computer access warrant cannot authorise the collection of evidence by interception for investigating an offence. If agencies require interception other than to facilitate a computer access warrant, they must seek an interception warrant from an eligible issuing authority under the TIA Act.

499. Paragraph 27E(2)(i) allows a computer access to authorise the doing of anything reasonably incidental to any of the things specified in paragraphs 27E(2)(a) to (h).

500. Subsection 27E(3) stipulates that data that is subject to some form of electronic protection is taken to be relevant for the purposes of determining whether it is relevant data covered by the warrant (subsection 27E(3) in association with paragraph 27E(2)(g)).

501. Subsection 27E(4) is a clarifying provision that reiterates the thresholds in section 27A which must be met before a law enforcement officer may apply for a computer access warrant.

Certain acts not authorised – 27E(5)

502. This subsection has the same effect as subsection 25A(5) of the ASIO Act. A computer access warrant does not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer. An exception to the limitation has been included so that an agency may undertake such actions where they are otherwise necessary to execute the warrant.

503. A computer access warrant cannot be used to disrupt or deny a service to a computer, even where that computer is being used for illegal purposes. Computer access warrants are evidence-gathering tools and are not intended to enable agencies to engage in disruption, or any activities which would generally be beyond the functions of the agencies.

504. However, subsection 27E(7) does permit an agency to do that which is necessary in order to conceal the fact that anything has been done under the warrant or under that subsection. This may include, for example, forcing a device to do a thing that disrupts its operation in order to conceal things done under the warrant.

Warrant must provide for certain matters – 27E(6)

505. A computer access warrant must authorise the use of force against persons or things that is necessary and reasonable to do the things specified in the warrant. Any unauthorised use of force against a person that does not comply with these requirements may attract criminal and civil liability. If the warrant authorises entry onto premises, then the warrant must state whether entry is authorised to be made at any time, or during a set period of time.

Concealment of access – 27E(7)

506. Subsection 27E(7) 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. Subsection 18(4) of the SD Act provides a similar provision in relation to surveillance device warrants. Likewise, under paragraph 25A(4)(c) of the ASIO Act, an ASIO computer access warrant authorises the doing of anything reasonably necessary to conceal the fact that anything has been done under the warrant.

507. Concealment of access is essential for preserving the effectiveness of covert warrants under the SD Act. Paragraphs 27E(7)(d) and (e) also authorise the entering of premises where the computer that has been accessed is located, or premises for gaining entry or access to where the computer is located, for the purposes of concealing the action that has been taken.

508. A computer access warrant may also authorise removing the computer or another thing from any place where it is situated, and returning it, for the purposes of concealing access. The ability to temporarily remove a computer from the premises is important in situations where an agency may have to use specialist equipment to access the computer but cannot for practical reasons bring that equipment onto the premises in a covert manner.

509. In some instances it will be necessary to retrieve a physically implanted computer access device from a computer in order for the access to be concealed. Doing anything

reasonably necessary for concealment as envisaged by paragraph 27E(7)(c) includes retrieving such a device.

510. Although there is a separate retrieval framework for surveillance devices upon expiry of a surveillance device warrant in the SD Act, retrieval provisions for computer access follows the structure of section 25A of the ASIO Act. This structure acknowledges the importance of ensuring that agencies have the ability to determine when access to premises or to a planted device will best ensure the operation remains covert. It will not always be possible to predict when safe retrieval of a device can be performed without compromising an investigation.

511. 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.

512. The period of time provided to perform these concealment activities recognises that, operationally, it is sometimes impossible to complete this process within 28 days of a warrant expiring. The requirement that the concealment activities be performed 'at the earliest time after the 28-day period at which it is reasonably practicable to do so' acknowledges that this authority should not extend indefinitely, circumscribing it to operational need.

27F - Extension and variation of computer access warrant

513. This section allows an officer to apply at any time while the warrant is in place for an extension of the warrant or a variation of its terms. This builds flexibility into the warrant process and accounts for extended investigations and unexpected circumstances. An application for extension may be made more than once. The application must be made to an eligible Judge or nominated AAT member. The Judge or member must consider the same matters required to issue a computer access warrant at first instance (see subsection 27C(2)) and be satisfied that the grounds on which the application for the warrant was made still exist (see subsection 27C(1)).

514. The provisions that apply to computer access warrants apply to varied or extended computer access warrants. This ensures that any varied specifications are within the bounds of what might have been authorised in a computer access warrant at first instance. For example, a varied computer access warrant must specify the list of things in subsection 27E(2). The warrant cannot authorise the addition, deletion or alteration of data that interferes with a person's use of a computer unless it is for the purposes of the warrant.

515. The warrant can only be extended for a period not exceeding 90 days from the day on which it would normally expire, but for the extension.

516. This provision does not prevent the issue of a further warrant in relation to the same investigation, applied for under section 27A.

27G - Revocation of computer access warrant

517. A computer access warrant may be revoked by an eligible Judge or nominated AAT member. If the warrant is revoked and the officer executing the warrant is already in the process of executing the warrant, the officer does not have any civil or criminal liability for actions done before he or she was made aware of the revocation.

518. The chief officer of the law enforcement agency to which the warrant was issued must revoke the warrant if satisfied that the warrant is no longer required for the purpose of enabling evidence to be obtained of the commission of the relevant offence for which it was obtained originally, or enabling evidence of the identity or location of the offender.

27H - Discontinuance of access under warrant.

519. Subsection 27H(2) places an obligation on the chief officer of a law enforcement agency to take steps to discontinue computer access where he or she is satisfied that the grounds on which a computer access warrant, issued in relation to a relevant offence, have ceased to exist. For example, the alleged offender may be in custody, so there would be no need to collect evidence of the location of the offender. Similarly, under subsection 27H(3) if the warrant was sought in relation to the recovery of a child and the chief officer of the agency is satisfied that the use of computer access to recover the child is no longer necessary, the chief officer must revoke the warrant. Subsection 27H(4) has the same effect but in relation to warrants sought for a mutual assistance authorisation. Subsection 27H(5) deals with integrity operations, and subsection 27H(6) relates to warrants sought for a control order.

520. Subsections 27H(7) and 27H(8) complement section 27G in that the chief officer must, if made aware that an issuing authority has revoked the warrant or a control order is no longer in force, take steps to discontinue computer access.

521. Subsections 27H(9) and 27H(10) places an obligation on the law enforcement officer who is primarily responsible for executing the warrant to immediately inform the chief officer if there is a change in circumstances affecting the warrant. This person will be in many cases the officer to whom the warrant was issued under section 27C and who made the application under section 27A. However, this may not always be the case as section 27A enables a person to apply for a warrant on behalf of the law enforcement officer. There may also be staffing and organisational changes during the period the warrant is in place. Subsection 27H(9) recognises that there may be multiple people working on the execution of a particular warrant, by placing the obligation on the person deemed primarily responsible. This position has not been legislated because agencies frequently structure investigations differently.

522. Upon being informed of the change in circumstances by the executing officer, the chief officer of the agency will have obligations under subsection 27H(2).

Item 50 – After subsection 28(1)

523. This item amends the emergency authorisation provisions in the SD Act to allow law enforcement officers to apply to an appropriate authorising officer (usually the head of the agency or deputy-head of the agency – see section 6A) for access to data held in computers in the course of an investigation of a relevant offence. New subsection 28(1A) provides that the law enforcement officer must suspect that there is an imminent risk of serious violence or substantial property damage, that access to the data in the target computer is immediately necessary for dealing with that risk, that the circumstances are so serious and the matter is so urgent that access to that data is warranted, and that it is not practicable to apply for a computer access warrant.

Item 51 – Subsections 28(2), (3) and (4)

524. This item amends subsections 28(2), (3) and (4) to account for the addition of subsection 28(1A) regarding emergency authorisations made for access to data in a computer where there is a serious risk to person or property.

525. Under subsection 28(2), a police officer of a State or Territory cannot apply for an emergency authorisation for State offences with a federal aspect as such offences are not to be included as a 'relevant offence' for the purposes of section 28. A police officer of a State or Territory can only apply for emergency authorisations to investigate Commonwealth offences.

526. Under subsection 28(3), such an application may be made orally, in writing, by telephone, email or fax or any other means of communication.

527. Subsection 28(4) provides that if the appropriate authorising officer is satisfied that there are reasonable grounds supporting the officer's suspicion of the matters in subsection 28(1), the authorising officer may give an emergency authorisation.

Item 52 – After subsection 29(1)

528. This item amends the emergency authorisation provisions in the SD Act to allow law enforcement officers to apply to an appropriate authorising officer (usually the head of the agency or deputy-head of the agency – see section 6A) for access to data held in computers in urgent circumstances relating to a recovery order. New subsection 29(1A) provides that the officer must suspect that the circumstances are so urgent as to warrant the immediate use of access to data held in the target computer.

529. The circumstances must also be such that it is not practicable to apply for a computer access warrant. The threshold in relation to a recovery order is slightly lower than for an investigation related to a relevant offence. There are three tests to satisfy in this instance because of the urgency and seriousness inherent in recovering a child.

Item 53 – Subsections 29(2) and (3)

530. This item is consequential to item 52 which inserts subsection 29(1A). This item amends subsections 29(2) and (3) regarding emergency authorisations made for access to data in a computer where there are urgent circumstances relating to a recovery order.

531. To issue an emergency authorisation, the authorising officer must be satisfied that there are reasonable grounds supporting the officer's suspicion that such an authorisation is required in paragraph 29(1)(b).

532. Under subsection 29(2), an application under this section is able to be made orally, in writing, by telephone, fax, email or other means of communication.

Item 54 – After subsection 30(1)

533. This item enables emergency authorisations to be made in regard to access to data held in a computer where there is a risk of loss of evidence. The provisions match the existing requirements and powers available for surveillance device emergency authorisations where there is a risk of loss of evidence under section 30.

534. A law enforcement officer will be able to apply for an emergency authorisation in an investigation for offences specified in subsection 30(1A) where that law enforcement officer reasonably suspects that the access to data in a computer is immediately necessary to prevent the loss of any evidence that is relevant to the investigation of the specific offence. The suspicion must be that the circumstances are so serious and the matter is of such urgency that access to data held in a computer is warranted and that it is not practical to apply for a computer access warrant.

535. Those offences in subsection 30(1A) are given special provision in the Act due to the recognised seriousness of these offences and/or the difficulty of obtaining evidence of their nature.

Item 55 – Subsection 30(2)

536. This item is consequential to item 54 which inserts subsection 30(1A). This item amends subsection 30(2) by inserting 'mentioned in subsection (1) or (1A)' after the word 'application' into section 30 regarding emergency authorisations made for access to data in a computer where there is a risk of loss of evidence.

537. This amendment also ensures that applications for an emergency authorisation made for access to data in a computer can be made orally, in writing, by telephone, fax, email or any other means of communication.

Item 56 – Subsection 30(3)

538. This item is consequential to item 54 which inserts subsection 30(1A). This item amends subsections 30(3) regarding emergency authorisations made for access to data in a computer where there is a risk of loss of evidence by omitting the word 'the' and substituting it with 'in the case of an application mentioned in subsection(1), the'.

539. This item is necessary as item 57 will insert a new subsection 30(4) that mirrors subsection 30(3).

Item 57 – At the end of section 30

540. This item is consequential to item 54 which inserts subsection 30(1A). This item inserts subsection 30(4) into section 30 regarding emergency authorisations made for access to data in a computer where there is a risk of loss of evidence.

541. Subsection 30(4) mirrors subsection 30(3) but applies to access to data in a computer rather than a surveillance device.

542. This item provides that an appropriate authorising officer may give an emergency authorisation in relation to the conduct of an investigation into a specified offence set out in subsection 30(1A), where the authorising officer is satisfied that the investigation is being conducted into an offence under subsection 30(1A), and there are reasonable grounds for the law enforcement officer's suspicion that access to data in a computer is necessary to prevent the loss of relevant evidence, the matter is serious and urgent and applying for a computer access warrant under the normal circumstances is not practicable.

Item 58 – Subsections 32(1) and (2)

543. This item is consequential to item 59 and 60 which insert new subsections 32(2A) and (3A). This item amends subsections 32(1) and (2) by inserting 'for the use of a surveillance device' after the word 'authorisation'.

Item 59 – After subsection 32(2)

544. This item inserts subsection 32(2A) into section 32. Subsection 32(2A) is similar to existing subsection 32(2) and applies to computer access.

545. Subsection 32(2A) provides that an emergency authorisation may authorise anything that a computer access warrant authorises.

Item 60 – After subsection 32(3)

546. This item inserts subsection 32(3A) into section 32. Subsection 32(2A) is similar to existing subsection 32(3) and applies to computer access.

547. Subsection 32(2A) provides that a law enforcement officer may only access data held in a computer if he or she is acting in performance of his or her duty.

Item 61 – Subsection 33(2)

548. This item is consequential to item 62 which inserts new subsection 33(2A). This item amends subsection 33(2) by omitting the word 'the' and substituting it with 'in the case of an application for an emergency authorisation for the use of a surveillance device, the'.

Item 62 – After subsection 33(2)

549. This item inserts new subsection 33(2A). Subsection 33(2A) provides that an application for an emergency authorisation for access to data held in a computer must specify the name of the applicant for the approval, and if a warrant is sought, the nature and duration of the warrant. The authorisation must be supported by an affidavit stating grounds for issue and be accompanied by a copy of the written record made under existing section 31 of the SD Act.

550. Subsection 33(2A) is similar to existing subsection 33(2), but will apply to access to data in a computer rather than a surveillance device.

Item 63 – Subsection 34(1)

551. This item amends subsection 34(1) and is consequential to item 64 which inserts new subsection 34(1A). This item omits the words 'section 28' and replaces it with "subsection 28(1)".

Item 64 – After subsection 34(1)

552. This item inserts subsection 34(1A) which sets out the considerations that a Judge or nominated AAT member must take into account before deciding whether to approve an emergency authorisation for computer access issued by an appropriate authorising officer under new subsection 28(1A), in circumstances where the law enforcement officer reasonably

suspects that there is an imminent risk of serious violence to a person or substantial damage to property.

553. The Judge or nominated AAT member must, being mindful of the intrusive nature of accessing data held in a computer, turn his or her mind to the following factors:

a. the nature of the risk of serious violence to a person or substantial damage to property

b. the extent to which issuing a computer access warrant would have helped reduce or avoid the risk

c. the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk

d. how much the use of such methods would have helped reduce or avoid the risk

e. how much the use of such methods would have prejudiced the safety of the person or property because of delay or for another reason, and

f. whether or not it was practicable in the circumstances to apply for a computer access warrant.

554. In considering these factors, the Judge or member stands in the shoes of the appropriate authorising officer at the time he or she made the decision to issue the emergency authorisation in light of the information that was available at the time of that decision. In this way, the Judge or member determines whether accessing data held in a computer without court approval was justified at the time, given the information that was before the appropriate authorising officer.

555. This subsection is similar to existing subsection 34(1), which sets out the considerations that must be taken into account before a Judge or member may approve emergency authorisation for the use of a surveillance device, in circumstances where the law enforcement officer reasonably suspects that there is an imminent risk of serious violence to a person or substantial damage to property.

Item 65 - Subsection 34(2)

556. This item makes a consequential amendment to reflect the inclusion of new subsection 29(1A) in section 29 in item 66. To facilitate this new subsection, current section 29 is amended to become subsection 29(1).

Item 66 – After subsection 34(2)

557. This item inserts subsection 34(2A) which sets out the considerations that a Judge or nominated AAT member must take into account before deciding whether to approve an emergency authorisation for computer access issued by an appropriate authorising officer under new subsection 29(1A), where a recovery order is in force.

558. The Judge or nominated AAT member must, being mindful of the intrusive nature of accessing data held in a computer, turn his or her mind to the following factors:

a. the urgency of enforcing the recovery order

b. the extent to which accessing data would assist in the location and safe recovery of the child to whom the order relates

c. the extent to which law enforcement officers could have used alternative methods to assist in the location and safe recovery of the child

d. how much the use of such methods would have might have prejudiced the effective enforcement of the recovery order, and

e. whether or not it was practicable in the circumstances to apply for a computer access warrant.

559. In considering these factors, the Judge or member stands in the shoes of the appropriate authorising officer at the time he or she made the decision to issue the emergency authorisation in light of the information that was available at the time of that decision. In this way, the Judge or member determines whether accessing data held in a computer without court approval was justified at the time, given the information that was before the appropriate authorising officer.

560. This subsection is similar to existing subsection 34(2), which sets out the considerations that must be taken into account before a Judge or member may approve emergency authorisation for the use of a surveillance device, where a recovery order is in force.

Item 67 – Subsection 34(3)

561. This item makes a consequential amendment to reflect the inclusion of new subsection 30(1A) in item 68. To facilitate this new subsection, current section 30 is amended to become subsection 30(1).

Item 68 – At the end of section 34

562. This item inserts subsection 34(4) which sets out the considerations that a Judge or nominated AAT member must take into account before deciding whether to approve an emergency authorisation for computer access issued by an appropriate authorising officer under new subsection 30(1A), in circumstances where the law enforcement officer is conducting an investigation into specified Commonwealth offences.

563. The Judge or nominated AAT member must, being mindful of the intrusive nature of accessing data held in a computer, turn his or her mind to the following factors:

a. the nature of the risk of the loss of evidence

b. the extent to which issuing a computer access warrant would have helped reduce or avoid the risk

c. the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk

d. how much the use of such methods would have helped reduce or avoid the risk, and

e. whether or not it was practicable in the circumstances to apply for a computer access warrant.

564. In considering these factors, the Judge or member stands in the shoes of the appropriate authorising officer at the time he or she made the decision to issue the emergency authorisation in light of the information that was available at the time of that decision. In this way, the Judge or member determines whether accessing data held in a computer without court approval was justified at the time, given the information that was before the appropriate authorising officer.

565. This subsection is similar to existing subsection 34(3), which sets out the considerations that must be taken into account before a Judge or member may approve emergency authorisation for the use of a surveillance device, in circumstances where the law enforcement officer is conducting an investigation into specified Commonwealth offences.

Item 69 – Section 35 (heading)

566. This item makes a consequential amendment to reflect the inclusion of new section 35A, which allows a Judge or nominated AAT member to approve emergency authorisation for access to data held in a computer. The item clarifies that existing section 35 allows a Judge or nominated AAT member to approve emergency authorisation for the use of a surveillance device.

Item 70 – Subsection 35(1)

567. This item makes a consequential amendment to reflect the inclusion of new subsection 28(1) in section 28.

Item 71 – Subsection 35(1)

568. This item omits 'approve the application,' and substitutes 'give the approval.'

Item 72 – Subsection 35(2)

569. This item makes a consequential amendment to reflect the inclusion of new subsection 29(1) in section 29.

Item 73 – Subsection 35(2)

570. This item omits 'approve the application,' and substitutes 'give the approval.'

Item 74 – Subsection 35(3)

571. This item makes a consequential amendment to reflect the inclusion of new subsection 30(1) in section 30.

Item 75 – Subsection 35(3)

572. This item omits 'approve the application,' and substitutes 'give the approval.'

Item 76 – After section 35

573. This item sets out the conditions on which an eligible Judge or nominated AAT member may approve an emergency authorisation in relation to investigating a relevant offence (subsection 35A(1)), enforcing a recovery order (subsection 35A(2)) or preventing the loss of evidence (subsection 35A(3)).

574. Before approving an emergency authorisation in relation to investigating a relevant offence, the eligible Judge or nominated AAT member must be satisfied of the grounds underlying the emergency authorisation. He or she must be satisfied that at the time the authorisation was given:

a. there was a risk of serious violence to a person or substantial damage to property

b. accessing data held in the target computer may have helped reduce the risk, and

c. it was not practicable in the circumstances to apply for a computer access warrant.

575. Similarly, before approving an emergency authorisation for the purposes of enforcing a recovery order, the eligible Judge or nominated AAT member must be satisfied that:

a. there was a recovery order in force at the time the authorisation was given, and

b. reasonable grounds existed to suspect that:

    i. the enforcement of the recovery order was urgent

    ii. accessing data held in the target computer may have assisted in the prompt location and safe recovery of the child, and

    iii. it was not practicable in the circumstances for a law enforcement officer to apply for a computer access warrant.

576. Before approving an emergency authorisation to prevent the loss of evidence, the eligible Judge or nominated AAT member must be satisfied that:

a. reasonable grounds existed to suspect that:

    i. there was a risk of loss of evidence

    ii. accessing data held in the target computer may have helped reduce that risk, and

b. it was not practicable in the circumstances for a law enforcement officer to apply for a computer access warrant.

577. Subsection 35A(4) sets out the options available to an eligible Judge or nominated AAT member when they have approved the giving of an emergency authorisation. Under paragraph 35A(4)(a) the Judge or member may issue a warrant for the continued access to the computer as if the application for the emergency authorisation were in fact an application for a computer access warrant under Division 4 of Part 2, provided that the activity that required

access continues to exist. The duration of the warrant is subject to a 90 day limit and the Judge or member is empowered to impose conditions or restrictions on the warrant.

578. Paragraph 35A(4)(b) provides that where the Judge or AAT member is satisfied that, since the application for the authorisation was made, the activity which required computer access has ceased, the Judge or member can make an order that the computer access cease.

579. Subsection 35A(5) provides the options where the eligible Judge or nominated AAT member chooses not to approve the giving of an emergency authorisation under new subsections 28(1A), 29(1A) and 30(1A) at subsections 35A(1),(2) and (3) respectively. In these circumstances, the Judge or member may order that computer access cease altogether. Where the Judge or member believes that the situation did not warrant an emergency authorisation at the time it was issued but that computer access under Division 4 of Part 2 has now become necessary, the Judge or member may issue a computer access warrant for subsequent access. In this case, the application for the approval of the emergency authorisation shall be treated as if it was an application for computer access warrant under Division 4 of Part 2.

580. Subsection 35A(6) provides that, in any case, the eligible Judge or nominated AAT member may order that any information obtained from or relating to the exercise of powers under an emergency authorisation or any record of that information be dealt with in a manner specified in the order. The Judge or member may not order that such information be destroyed because such information, while improperly obtained, may still be required for a permitted purpose, such as an investigation. Division 5 of the Act governs what can be done with such information.

Item 77 – Section 36

581. This item makes a consequential amendment to reflect the inclusion of new section 35A, differentiating section 35 from new section 35A within section 36.

Item 78 – Section 41 (definition of *appropriate consenting official*)

582. This item repeals and substitutes the definition of appropriate consenting official so that it means an official of a foreign country with the authority to give consent to either the use of surveillance devices in that country or on a vessel or aircraft of that country, or to access to data held in computers in that country or on a vessel or aircraft.

Item 79 - Section 42 (heading)

583. This is a consequential amendment limiting the application of section 42 to surveillance device warrants. Sections 43A and 43B provide for the extraterritorial operation of computer access warrants.

Item 80 - Subsection 42(1)

584. This is a consequential amendment limiting the application of section 42 to surveillance device warrants.

Item 81 - After paragraph 42(2)(a)

585. This is a consequential amendment limiting the application of subsection 42(2) to emergency authorisations issued in respect of surveillance devices.

Item 82 - Paragraph 42(2)(b)

586. This is a consequential amendment limiting the application of subsection 42(2) to emergency authorisations issued in respect of surveillance devices.

Item 83 - Subsection 42(2)

587. This is a consequential amendment limiting the application of subsection 42(2) to emergency authorisations issued in respect of surveillance devices.

Item 84 – Subsection 42(2)

588. This is a consequential amendment limiting the application of subsection 42(2) to emergency authorisations issued in respect of surveillance devices.

Item 85 - Paragraph 42(3)(a)

589. This is a consequential amendment limiting the application of paragraph 42(3)(a) to emergency authorisations issued in respect of surveillance devices.

Item 86 - Subsections 42(6) and (9)

590. This is a consequential amendment limiting the application of subsections 42(6) and (9) to emergency authorisations issued in respect of surveillance devices.

Item 87 - At the end of Part 5

591. Part 5 of the SD Act provides for how surveillance device warrants operate extraterritorially. If in the course of an investigation a law enforcement agency needs to place a surveillance device in a foreign country or on a vessel or aircraft beyond Australia's territorial waters that is registered under the law of a foreign country, the agency must have the permission of a foreign official of that country. This only applies to federal law enforcement officers. State and Territory officers may not engage in extraterritorial surveillance (section 42). In this way, extraterritorial surveillance is carried out under an Australian warrant, with the agreement of the foreign State, which ensures that such surveillance is subject to appropriate accountability and probity measures under domestic law.

592. The same principle will apply to access to data held in a computer in a foreign country or on a vessel or aircraft that is registered under the law of a foreign country and is in waters beyond Australia's territorial sea. For example, a suspect who has a computer located in Australia may have data stored overseas, such as in cloud storage or in an email account for which the server is hosted in a foreign country. In this instance, the law enforcement officer conducting the investigation would have to seek the consent of an appropriate foreign official in order for the warrant to be granted. This principle only applies to warrants and authorisations issued under the SD Act. It is not intended that this should be read in regard to powers under the Crimes Act, which are overt in nature.

593. If a computer access warrant has already been granted by the issuing authority and during the course of executing that warrant it becomes apparent that there will be a need for access to data held in a computer in a foreign country (or on a foreign vessel or aircraft) the warrant is taken to permit that access if the access has been agreed to by an appropriate consenting official of the foreign country. This means that a law enforcement officer does not need to seek a further warrant, or a change in the warrant conditions from the issuing authority, as long as consent from the foreign official has been granted.

594. For clarity, the application of computer access warrants extraterritorially to vessels registered under the law of a foreign country is not intended to conflict with sovereign immunity that is provided, for example, to visiting warships of a foreign nation.

595. In the course of computer access as a result of an emergency authorisation, the law enforcement officer will have to seek a warrant from an eligible Judge or AAT member upon determining that access to data held in a computer in a foreign country will be necessary. The Judge or AAT member cannot issue the warrant unless satisfied that the access has been agreed to by an appropriate consenting official of the foreign country.

596. The chief officer of the law enforcement agency that applied for the warrant belongs or is seconded, must give the Attorney-General written evidence that the surveillance has been agreed to by an appropriate consenting official of the foreign country. The chief officer is to provide this evidence of consent as soon as practicable after the access to data has commenced under a warrant in a foreign country or on a foreign vessel or aircraft where such consent is required. An instrument providing evidence to the Attorney-General is not a legislative instrument. It is administrative rather than legislative in character. It does not determine or alter the law but instead is an instrument relating to a specific situation and serving a specific operational purpose.

597. In some instances the consent of a foreign official is not required notwithstanding the fact that the data may be held in a computer offshore. Where the person executing the warrant is physically present in Australia and the location of the data is unknown, or cannot reasonably be determined, the consent of a foreign official is not required.

598. Persons of interest to law enforcement may use email accounts and messaging platforms provided by technology companies with international reach. The data associated with these services is increasingly stored in offshore data centres. Data about one account may be held in multiple data centres at any one time and data may move between different centres. Sometimes data may only be held in one place for a days or a few hours. This frequently makes the location of data unknowable or indeterminable.

Item 88 – Subsection 44(1) (after paragraph (a) of the definition of *protected information*)

599. Information obtained pursuant to surveillance device powers under the Act is protected by restrictions on use, communication and publication in Part 6. The Act operates by first defining that information as ‘protected information’ under section 44, prohibiting the use and disclosure of that information in certain circumstances in section 45, and providing for some exceptions.

600. Item 88 deems information obtained from access to data either under a computer access warrant or under an emergency authorisation for access to data ‘protected information’

in the same way that information obtained from the use of surveillance device is protected information. General computer access intercept information is not protected information for the purposes of the Act.

601. There are no amendments to current section 45, which contains the prohibitions on use, recording, communication or publication of protected information. As section 45 refers to 'protected information' as listed in section 44, amending the section 44 is sufficient to capture information relating to computer access.

602. Section 45 contains two offences. Under a subsection 45(1), s person cannot use, record, communicate, publish or admit into evidence protected information that does not fall into any of the exceptions in section 45. The penalty for doing so is a maximum of 2 years imprisonment. Section 45(2) is a more serious offence where dealing with the information endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence. The penalty is a maximum of 10 years imprisonment.

603. The exceptions to this prohibition are contained in subsection 45(5). They include the investigation of a relevant offence, the making of a decision to prosecute for a relevant offence, an investigation into the conduct or a public officer, making a decision in relation to the appointment of a public officer, and keeping records and undertaking inspections.

Item 90 – Subsection 44(1) (at the end of subparagraph (d)(iii) of the definition of *protected information)*

604. Item 90 is a consequential amendment allowing paragraph 44(1)(d) to continue to subparagraph 44(1)(d)(iv).

Item 91 - Subsection 44(1) (after subparagraph (d)(iii) of the definition of *protected information*)

605. Item 91 provides that where information has been obtained through access to data held in a computer in a foreign country, or on a vessel or aircraft of a foreign country, without the agreement of a consenting official, that information is classified as protected information.

Item 91A – Subsection 44(1) (at the end of the definition of protected information)

606. Item 91A adds a note pointing to Part 2-6 of the TIA Act, which contains protections for general computer access intercept information.

Item 92 – Section 46 (heading)

607. This item is a consequential amendment to section 46 in order to reflect the inclusion of computer access warrants within the SD Act.

Item 93 – Paragraph 46(1)(a)

608. This item ensures that general computer access intercept information, although not protected information, has record keeping requirements. The chief officer of a law enforcement agency must ensure that general computer access intercept information is kept in a secure place that is not accessible to people who are not entitled to deal with that information. He or she must also cause the information to be destroyed as soon as practicable once it is no longer required.

Item 94 – Subsection 46(2)

609. This amends subsection 46(2) to reflect the inclusion of computer access warrants within the SD Act. It is a consequential amendment.

Item 95 – After subsection 46A(1)

610. This item inserts new subsection 46A(1A) which contains requirements for causing a record or report obtained from access to data relating to a control order warrant to be destroyed, where the information has been obtained before a control order came into force. If the chief officer of an agency is satisfied that the information is no longer likely to assist in connection with the protection of the public from a terrorist act, preventing the provision of support for or the facilitation of a terrorist act, or preventing the provision of support for or facilitation of engagement in a hostile activity in a foreign country, he or she must cause the record or report to be destroyed as soon as practicable.

Item 96 – Subsection 46A(2)

611. This item is a consequential amendment clarifying that as section 6C of SD Act does not apply to 46A(1) neither does it apply to 46A(1A).

Item 97 - After section 47

612. This item inserts new section 47A. Section 47A gives protection to sensitive information relating to computer access technologies and methods in order to prevent its release into the public domain. Releasing such information could harm future capabilities and investigations. Section 47 is a protection additional to other statutory protections such as public interest immunity. Section 47A replicates section 47, which provides protections for surveillance technologies and methods. This section is intended to protect technologies that develop over time and not to limit law enforcement agencies with an exhaustive list.

613. Subsection 47A(1) provides that a person may object to the disclosure of information on the ground that the information could reasonably be expected to reveal details of computer access technologies or methods. It is not intended that section 47A could give protection to simple aspects of computer access, such as the action of turning on a computer or the fact that a computer was turned on. The section is for sensitive technologies and methods that need to be closely held. However these are not excluded explicitly from section 47A because it is within the discretion of the person presiding over the proceeding whether information is of sufficient sensitivity (subsection 47A(2)).

614. Subsection 47A(3) requires the person presiding over the proceeding to take into account whether disclosure of the information is necessary for the fair trial of the defence and whether it is in the public interest. This ensures that the availability of capability protection for law enforcement is not absolute. The public interest in protecting sensitive operational and capability information must be weighed against the defendant's right to a fair trial and other public interests.

615. Subsection 47A(4) is a saving provision which provides that this section does not affect any other law under which a law enforcement officer cannot be compelled to disclose information or make statements in relation to the information.

616. Subsection 47A(5) requires the person presiding over the proceeding to make any order they consider necessary to protect computer access technologies or methods that have been disclosed from being published. This does not apply if doing so would conflict with the interests of justice (subsection 47A(6)). It is appropriate to protect this information without a requirement to consider harm or that the disclosure of the information would be contrary to the public interest. It is assumed that disclosure is inherently harmful. Law enforcement capabilities are fundamental to ongoing investigations and their ability, including over the long-term, to protect essential public interests, including national security and public safety.

617. Subsection 47A(7) provides the definition of computer access technologies or methods, as technologies or methods relating to using a computer, a telecommunications facilities, any other electronic equipment, or a data storage device, for the purposes of obtaining access to data, or for adding, copying, deleting or altering other data in a computer. These activities must have been deployed in giving effect to a warrant or an emergency authorisation.

Item 98 – Subsection 49(2)

618. This is a consequential amendment limiting the application of subsection 49(2) to emergency authorisations for surveillance devices or tracking device authorisations.

Item 99 – After subsection 49(2A)

619. This item provides the reporting requirements relating to computer access warrants and emergency authorisations. There is no amendment to subsection 49(1) as the current language would apply to computer access warrants and emergency authorisations granted for computer access. That subsection states that the chief officer of a law enforcement agency must make a report to the Minister and give a copy of each warrant and authorisation to the Minister.

620. Subsection 49(2B) lists the requirement of the report. The report must state whether the warrant or authorisation was executed, the name of the person primarily responsible for the execution, the name of each person involved in accessing data, the name of any person whose data was accessed, and the location at which the computer was located. The report must also give details of the benefit to the investigation of a relevant offence, child recovery operation, integrity operation (as applicable).

621. Where the computer warrant is a control order access warrant, the report must detail the use to be made of any evidence or information obtained by accessing data and the benefit of accessed data in:

a. protecting the public from a terrorist act

b. preventing the provision of support for, or the facilitation of, a terrorist act

c. preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or

d. determining whether a control order has been or is being complied with.

The reporting requirements recognise that accessing a person’s data under a computer access warrant is a privacy intrusive measure, which requires proportionate safeguards.

Item 100 – Subsection 49A(1)

622. This item ensures that within six months after a warrant for computer access relating to a control order is issued, the chief officer of the agency must notify the Commonwealth Ombudsman that the warrant has been issued and must give the Commonwealth Ombudsman a copy of the warrant.

Item 101 – Paragraph 49A(2)(a)

623. If any conditions in a control order access warrant are contravened the chief officer of the relevant agency must notify the Commonwealth Ombudsman of that contravention as soon as practicable.

Item 102 – After paragraph 49A(2)(b)

624. If the chief officer of the law enforcement agency fails to revoke a control order warrant once it is no longer required (therefore contravening subsection 27G(2)), the chief officer of the relevant agency must notify the Commonwealth Ombudsman as soon as practicable.

Item 103 – After paragraph 49A(2)(c)

625. If a law enforcement officer uses, records, communicates or publishes protected information obtained under a control order access warrant (therefore committing an offence under section 45), the chief officer of the agency must notify the Commonwealth Ombudsman of that contravention as soon as practicable.

626. If a law enforcement officer fails to keep in a secure place or destroy information obtained under a control order access warrant as required under section 46(1), the chief officer of the relevant agency must notify the Commonwealth Ombudsman as soon as practicable.

Item 104 – Subsection 49A(3)

627. A failure to report to the Commonwealth Ombudsman on the issuing of the control order access warrant or about a contravention of such a warrant does not affect the validity of a control order access warrant.

Item 105 – Paragraphs 50(1)(g), (h) and (i)

628. Section 50 of the SD Act sets out the reporting requirements agencies have to meet each financial year in their annual report to the Minister. Agencies must report on the number of warrants applied for and issued during the year and the number of emergency authorisations. The report must also specify the number of warrants and authorisations that were refused in the year and the reasons for their refusal. The report is to be submitted to the Minister as soon as practicable, within a three month period, following the end of each financial year (subsection 50(3)).

629. This item ensures that these reporting obligations apply to computer access warrants and authorisations as well as those relating to surveillance devices. As such paragraphs (g),

(h) and (i) which specifically state 'the use of a surveillance device under a warrant' are amended so as not to be limited to those types of warrants.

Item 106 – Paragraph 50(1)(j)

630. The annual report must include any other information relating to the use of surveillance devices or access to data held in computers that the Minister considers appropriate.

Item 107 – Subsection 50A(6) (definition of *control order information*)

631. This item repeals the definition of control order information and substitutes a definition which takes into account the new computer access warrants in the Act.

Item 108 – Paragraph 51(b)

632. This item ensures that each instrument of revocation including those issued under new subsection 27G(4) must be kept by the agency.

Item 109 – Paragraphs 52(1)(e), (f), (g) and (h)

633. Section 52 lists the other records that the chief officer of an agency is required to ensure are kept. They relate to the decision to grant, refuse or withdraw warrants and authorisations, as well as records relating to the use and communication of information obtained under warrants.

634. This item amends subsection 52(1) to provide that the chief officer of a law enforcement agency must cause this information relating to computer access to be kept.

Item 110 – Paragraph 52(1)(j)

635. This is item ensures that details of destruction of records or reports relating to computer access must also be kept.

Item 111 – After subparagraph 53(2)(c)(iiic)

636. Section 53 requires agencies to maintain a register of warrants and authorisations. The purpose of the register is to provide an overview for the Commonwealth Ombudsman when inspecting such records under Division 3 of the Act. This items ensures that control order access warrants kept on the register include the date the control order was made.

Item 112 – At the end of subsection 62(1)

637. An appropriate authorising officer, or a person assisting him or her, may issue a written certificate setting out the facts of what has been done by the law enforcement officer or a person providing technical expertise in connection with the execution of the warrant or the emergency authorisation. The statement can also set out anything done by the officer in connection with communicating information, making use of, or making a record of information. Evidentiary certificates are intended to streamline the court process by reducing the need to contact numerous officers and experts to give evidence on routine matters. Evidentiary certificates also assist agencies to protect sensitive capabilities.

638. This item ensures that certificates can be issued in respect of anything done by the law enforcement officer in connection with the communication, making use of, making a record of or the custody of a record of information obtained from access to data.

Item 113 – Subsection 62(3)

639. This is a consequential amendment to take into account the insertion of section 35A in respect of emergency authorisations. Subsection 62(3) provides that evidentiary certificates are not admissible in evidence in any proceedings to the extent the certificate sets out facts with respect an emergency authorisation unless the authorisation has been approved.

Item 114 – After section 64

640. A law enforcement officer may apply to an eligible Judge or AAT member for an order requiring a specified person to provide any information or assistance is that reasonable and necessary to allow the law enforcement officer to access data held in a computer subject to a computer access warrant. This provision is similar to section 3LA of the Crimes Act, which allows a constable to apply to a magistrate for an order requiring a person to provide assistance where a search warrant is in place.

641. This item ensures that law enforcement agencies that have a warrant for computer access will be able to compel assistance in accessing devices. Although the SD Act provides for the issuing of warrants permitting covert activity, there may be circumstances in the course of an investigation where a person who is not the suspect or target will have knowledge of a computer system and be able to provide access to relevant data, without compromising the covert nature of the investigation. Alternatively, there may be a point in the investigation where the benefits of compelling information from a person in order to enable access to data outweigh the disadvantages of maintaining the secrecy of the investigation.

642. There are limits to when an eligible Judge or AAT member may grant the assistance order. Where the order relates to a computer access warrant issued, or authorisation given, with respect to a relevant offence, the Judge or AAT member must be satisfied that there are reasonable grounds for suspecting that access to data is necessary in the course of the investigation to enable evidence of the commission of the offences or identity or location of the offenders. The Judge or AAT member must be satisfied that the person specified in the order is either:

a. reasonably suspected of having committed any of the offences to which the warrant or emergency authorisation relates

b. the owner or lessee of the computer or device

c. an employee of the owner or lessee of the computer or device

d. a person engaged under a contract for services by the owner or lessee of the computer or device

e. a person who uses or has used the computer or device, or

f. a person who is or was a system administrator for the system including the computer or device.

643. The specified person must also have relevant knowledge of the computer or measures applied to protect data held in the computer.

644. The Judge or AAT member must take into account similar considerations for orders relating to child recovery, mutual assistance, control orders and the protection of evidence.

645. The penalty for not complying with a request compelling assistance under section 64A is a maximum of imprisonment for 10 years. This is consistent with the amended penalty in Schedule 3 for committing the aggravated offence under amended subsection 3LA(5) of the Crimes Act. There is no equivalent five year penalty for the simple offence in the Crimes Act because there are no equivalent simple offences under the SD Act, that is, offences which carry a penalty of less than a maximum of three years imprisonment are not investigated under the SD Act.

Item 115 – After subsection 65(1)

646. Section 65 provides that if there is a defect or irregularity in relation to the warrant or emergency authorisation and but for that defect or irregularity the warrant or authorisation would be sufficient authority for the use a surveillance device in obtaining information or a record, then the use of the device is to be treated as valid, and the information or record can be given in evidence.

647. This item ensures that the same is the case for information or a record obtained pursuant to a computer access warrant or a computer access emergency authorisation, were a defect or irregularity to be found.

Item 116 – Subsection 65(2)

648. This item ensures that subsection 65(2) applies to defects and irregularities in relation to surveillance device warrants and surveillance device emergency authorisations and also to computer access warrants and authorisations. Under this subsection, a defect or irregularity means:

a. in or in connection with the issue of a document purporting to be a warrant or authorisation, or

b. in connection with the execution or purported execution of the warrant or authorisation (or document purporting to be a warrant or authorisation).

649. A defect or irregularity does not mean a substantial defect or irregularity.

Item 117 – After subsection 65A(2)

650. This item provides that a person is not criminally liable for any actions done under a control order access warrant issued on the basis of an interim control order where the interim order is subsequently declared to be void. This item replicates the existing provisions for control orders.

Item 118 – Section 65B (heading)

651. This item repeals the heading in 65B to account for 65B now providing for both control order warrants and control order access warrants.

Item 119 – After subparagraph 65B(1)(a)(i)

652. If a control order access warrant was issued on the basis of an interim control order, and a court subsequently declares that the interim order is void, any information obtained under the warrant can be used, communicated or published if the person reasonably believes that doing so is necessary for preventing or reducing the risk of the commission of a terrorist act or serious harm to a person or property.

Telecommunications Act 1997

Item 119A – After paragraph 313(7)(c)

Section 313 of the Telecommunications Act provides an obligation for carriers and carriage service providers to give agencies 'such help as is reasonably necessary' to enforce the criminal law and safeguard national security. New paragraph 313(7)(caa) ensures that 'giving help' includes giving effect to authorisations to develop and test interception capabilities under section 31A of the TIA Act.

Telecommunications (Interception and Access) Act 1979

Item 120 – Subsection 5(1)

653. Items 120 to 131 contain the amendments being made to the TIA Act to facilitate ASIO or a law enforcement agency being able to undertake limited interception in order to execute a computer access warrant. For technical reasons, an agency may have to intercept communications for the purposes of executing a computer access warrant. New paragraph 27E(2)(h) of the SD Act and new paragraph 27E(2)(e) of the ASIO Act permit intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing anything specified in the computer access warrant.

654. Item 120 inserts 4 definitions into section 5 of the TIA Act.

655. *ASIO computer access intercept information* means information obtained under the listed sections in the ASIO Act by intercepting a communication passing over a telecommunications system. This is distinct from information under a computer access warrant granted to ASIO by using computer access.

656. *ASIO computer access warrant* means a warrant issued under the listed provisions in the ASIO Act.

657. *General computer access intercept information* means information obtained under a general computer access warrant by intercepting a communication passing over a telecommunications system. This is distinct from information obtained under a computer access warrant by executing computer access itself. The permissible uses of data, information and records obtained through computer access are governed by the SD Act.

658. *General computer access warrant* means a warrant issued under section 27C of the SD Act, which is the provision specifying how an issuing authority can make a determination to issue a warrant for computer access.

Item 121 - Subsection 5(1) (at the end of the definition of restricted record)

659. This item excludes general computer access intercept information from the definition of restricted record. The purpose is to ensure that agencies in possession of original general computer access intercept information are not subject to the obligations imposed by the TIA Act relating to those records. Instead, record management will be governed by the SD Act.

Item 122 – Subsection 5(1) (paragraph (b) of the definition of *warrant*)

660. This item adds general computer access warrants and ASIO computer access warrants to the definition of 'warrant' in the TIA Act. The effect of this amendment is that interception for the purposes of either of these warrants is not prohibited. ASIO and law enforcement agencies will at times need to intercept information in order to execute computer access warrants.

661. Under subsection 7(1) of the TIA Act, interception of a communication passing over a telecommunications system is prohibited. Subsection 7(2)(b) provides the relevant exception; the prohibition does not apply in relation to interception of a communication under a warrant.

Item 123 - After paragraph 7(2)(b)

662. This item provides additional exceptions to the prohibition in subsection 7(1) of the TIA Act against interception of a communication passing over a telecommunications system. This ensures that intercepting communications to execute a computer access warrant under the ASIO Act and SD Act is lawful.

663. Under paragraph 7(2)(ba), the interception of a communication under subsections 25A(4) or (8), 27A(1) or (3C), or 27E(2) or 27E(6) of the ASIO Act is permitted.

664. Under paragraph 7(2)(bb), the interception of a communication under subsection 27E(7) of the SD Act is permitted.

Item 123A – Subsection 31(1)

665. This item amends subsection 31(1) of the TIA Act to permit the head of a security authority to request the Attorney-General to authorise the security authority to work with a carrier in order to test or develop interception technologies. Currently, subsection 31(1) only allows testing by employees of a security authority.

666. This amendment is not intended to, in any way, impact or read down current testing arrangements between security authorities or law enforcement agencies and carriers under the exception to the prohibition on interception in paragraph 7(2)(ab) of the TIA Act.

667. This item provides a route for security authorities to conduct their testing, or the testing of other interception agencies, with the assistance of carriers. The current exception to the prohibition to interception in paragraph 7(2)(ab) is restrictive in allowing testing only in relation to 'the installation, connection or maintenance of equipment used, or to be used, for the interception of communications under warrants.' It is sometimes necessary for agencies to test in ad hoc circumstances.

668. A request under subsection 31(1) may specify any number of carriers or carriage service providers to be covered by the authorisation. However, a request is not required to

specify a carrier if the security authority can undertake the testing without assistance. The head of the security authority can request multiple authorisations, which include any combination of carriers.

Item 123B – Subsection 31A(1)

669. Amendments to subsection 31A(1) will enable the Attorney-General, upon receiving a request, to authorise a security authority to work with a carrier to test interception technologies. The authorisation must be in writing and specify the period for which it will have effect. Authorisations cannot be made for a period greater than six months.

Item 123BA – After subsection 31A(4)

670. This item clarifies that although an authorisation may allow employees of the security authority and employees of the carrier to test interception technologies, this does not mean that the testing must involve one or more of the employees acting together at the same time. They do not need to be in one another's presence. For example, it is permissible for a carrier to undertake some activities related to testing, and then hand information to the security authority to undertake other activities. An officer of the security authority is not required to be present during any phase of testing activities

671. Use and disclosure of information obtained under an authorisation is discussed further in item 124A.

Item 123C – After subsection 31A

672. New section 31AA contains notification requirements where the Attorney-General has issued an authorisation for carriers to test interception technologies with a security authority.

673. The head of the security authority must give carriers named in an authorisation a copy of the authorisation as soon as practicable. There is no obligation on the head of security to provide advance notification to a carrier of the issue of an authorisation, ahead of providing a copy of the authorisation.

674. If an authorisation is varied or revoked, the head of the security authority must notify the carriers specified in the authorisation immediately. A copy of the variation or revocation must be given as practicable.

Item 123D – At the end of Part 2-4

675. This item inserts new section 31E to clarify that both an ASIO employee and ASIO affiliate are taken to be employees of ASIO.

676. A staff member of an agency in the IS Act, that is also a security authority, is taken to be an employee of the security authority. Agency is defined in the IS Act to mean ASIS, the Australian Geospatial-Intelligence Organisation (AGO) or ASD. A security authority is defined in the TIA Act as a Commonwealth authority that has functions primarily relating to security, the collection of foreign intelligence, the defence of Australia or the conduct of Australia's international affairs.

Item 124 – After section 63AA

677. The use, recording and communication of information obtained in the course of intercepting a communication in order to execute a computer access warrant is restricted. This is to ensure that where agencies want to gain intercept material for its own purpose, they must apply for, and be issued with, an interception warrant under Chapter 2 of the TIA Act.

678. This item inserts new section 63AB to provide two exceptions to the general prohibition on dealing in computer access intercept information.

679. Section 63AB allows a person, for the purposes of doing a thing authorised by a general computer access warrant, to communicate to another person, make use of, make a record or, or give in evidence in a proceeding general computer access intercept information. The intention is that intercepted information can be used or communicated for a purpose reasonably incidental to the purposes of carrying out computer access.

680. Section 63AB also allows a person to communicate general computer access intercept information to another person or make use or a record of that information if the information relates to involvement of a person in activities that, generally, exist in life threatening or emergency situations. These include:

a. activities that present a significant risk to a person's safety, or a threat to security
b. acting for or on behalf of a foreign power
c. activities that pose a risk to the operational security of ASIO, ASIS, AGO or ASD
d. activities that relate to the proliferation of weapons of mass destruction, and
e. activities that relate to a contravention by a person of a UN sanction enforcement law.

681. In these very serious circumstances, a person may communicate, use or record intercept information that would otherwise be prohibited.

682. New section 63AC replicates the exceptions in section 63AB for persons dealing with intercept material under the authority of an ASIO computer access warrant.

Item 124A – At the end of section 63B

683. This item provides the use and disclosure provisions of testing and development information obtained under a section 31A authorisation for employees of a carrier.

684. Employees of the carrier can gather, record and use the test and development information and may also communicate the information to employees of the security authority who sought the authorisation as well as other employees of the same carrier or employees of another carrier listed in the authorisation. Should it be required that a carrier provide information to another carrier, that second carrier (or any subsequent carrier) is subject to the same conditions in subsection 63B(5), being that the subsequent carrier may record or use the information and may share the information on to the security authority or another carrier in its original format or in a modified format. This is to ensure that if a daisy-chain style test is required (recognising that modern communications information may

pass over a number of systems), there are no impediments to the use and disclosure of information.

685. The limitation remains that the use and disclosure must be related to a testing or development purpose. A carrier is not to use the information provided to it or gathered by it for any other purpose.

686. Information collected under an authorisation may be retained for subsequent authorisation periods, should a subsequent authority require use of that information for the same purposes. This would include long term testing, where testing requires a baseline for comparison or where testing commenced in one testing authorisation period and completed in a subsequent testing authorisation period. Where the information is no longer required, it should be destroyed.

Item 125 – Paragraph 64(1)(a)

687. Item 125 constrains the permitted dealing of ASIO computer access intercept information. It ensures that ASIO computer access intercept information is not permitted to be communicated, made use of, or recorded even if in connection with the performance by ASIO of its functions or the performance of the IGIS of his or her functions, or for the purposes of security.

Item 126 – Paragraph 65(1)(a)

688. This item ensures that the Director-General of Security may not communicate to another person ASIO computer access intercept information, even if in accordance with subsections 18(3), (4A), or 19A(4) of the ASIO Act.

Item 126AA – At the end of section 65 (after the note)

689. This item provides limitations on the use and disclosure of testing and development information acquired under an authorised in section 31A of the TIA Act (Part 2-4) for security authorities.

690. Generally, sharing of testing and development information acquired under a section 31A authorisation is not permitted unless it is for testing and development purposes. Where the purpose is to share information to test and develop capabilities or analysis systems or support systems related to those systems, ASIO may share the information with a staff member of an authority of the Commonwealth or a State, ASD, ASIS, AGO, or a body listed in paragraph 19A(1)(d) or (e) of the ASIO Act. This can be for testing purposes of the receiving agency or for the testing purposes of ASIO.

691. This provision is intended to allow ASIO to undertake lead role functions in relation to testing interception capabilities and associated systems. ASIO is under no obligation to test or facilitate testing on behalf of permitted agencies listed above, but may do so at the request of permitted agencies.

692. Information generated by those permitted agencies under section 31A can be shared with ASIO for testing and development purposes. This is true irrespective of whether the section 31A authorisation was sought by, executed by or named ASIO.

Item 126A – Paragraph 65A(1)(a)

693. This provision is a consequential to limit the use of information obtained under a section 31A authorisation to develop or test technologies or interception capabilities. See item 126AA for substantive detail on use and disclosure provisions relevant to agencies.

Item 127 – Paragraph 67(1)(a)

694. Under section 67, an officer or staff member of an agency may, for a permitted purpose in relation to the agency, communicate to another person, make use of, or make a record of lawfully intercepted information and interception warrant information.

695. This item ensures that general computer access intercept information is not able to be communicated, made use of or recorded for these purposes.

Item 128 – Section 68

696. Under section 68, the chief officer of an agency may communicate lawfully intercepted information under certain circumstances. This item excludes general computer access intercept information from section 68.

Item 129 – Subsection 74(1)

697. Under section 74, a person may give lawfully intercepted information in evidence in an exempt proceeding.

698. This item ensures that a person may not give general computer access intercept information or ASIO computer access intercept information in evidence in an exempt proceeding.

Item 130 – Subsection 75(1)

699. Under section 75, a person may give information that has been intercepted in contravention of the prohibition in subsection 7(1) in evidence in an exempt proceeding.

700. This item ensures that a person may not give general computer access intercept information or ASIO computer access intercept information in evidence in an exempt proceeding.

Item 131 – Paragraph 77(1)(a) and (b)

701. This item provides that intercept material is admissible in evidence in so far as new sections 63AB and 63AC permit. Those sections permit the dealing of general computer access intercept information and ASIO computer access information where very serious circumstances exist or where there is a purpose reasonably incidental to the purposes of carrying out computer access.

Item 131A – After paragraph 108(2)(ca)

702. This item inserts new paragraph 108(2)(cb) provides an exception to the prohibition in subsection 108(1) on accessing a stored communication. The prohibition does not apply to accessing a stored communication under a general computer access warrant.

Part 2 – Application provisions

Item 132 – Application---computer access warrants

703. This Part contains application provisions for computer access warrants.

704. All amendments made under the provisions of this Schedule apply only to warrants, authorisations and orders issued after the commencement, being the day after the Bill receives the Royal Assent.

Part 3—Amendments contingent on the commencement of the Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2017

705. Schedule 2, Part 3 is to commence the later of a) immediately after the commencement of Schedule 2, Part 1 or b) immediately after the commencement of Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*. If the events of paragraph b) do not occur then Schedule 2, Part 3 is not to commence.

International Criminal Court Act 2002

Item 133 - After Division 12A of Part 4

706. This item inserts a new section which enables the Attorney-General to authorise applications for computer access warrants under the SD Act when a request is received from the International Criminal Court.

707. New subsection 79B(1) sets out the criteria that must be satisfied before the Attorney-General may authorise an application for a computer access warrant, including that the International Criminal Court has made a request in relation to access to data held in a computer, that the Attorney-General is satisfied that an investigation is being conducted by the Prosecutor, or a proceeding is before the International Criminal Court, and that the International Criminal Court has given appropriate undertakings on use of data, destruction of information and any other matters that the Attorney-General thinks appropriate.

708. New subsections 79B(2) and (3) clarify the scope and meaning of terms used in subsection (1). For consistency, the definitions are the same as in the SD Act.

709. The amendment enables Australian authorities to use the new computer access warrants to obtain information on behalf of the International Criminal Court pursuant to a request. This is consistent with the approach taken to requests for mutual legal assistance from foreign countries as set out in new section 15CC of the MACMA.

710. The threshold requirements under the SD Act will apply when an application is made.

711. Commencement of this item is subject to commencement of Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*. Subject to those provisions commencing, this item will commence immediately after the commencement of Part 1 of Schedule 2 of this Act or commencement of Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*, whichever is the latter. Part 6 of Schedule 1 of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*

inserts provisions that ensure that Australia is able to provide the same level of assistance to the International Criminal Court as can be provided to foreign countries under the MACMA.

International War Crimes Tribunals Act 1995

Item 134 - After Division 1A of Part 4

712. This item inserts a new section which enables the Attorney-General to authorise applications for computer access warrants under the SD Act that are requested by a Tribunal established under the *International War Crimes Tribunals Act 1995*.

713. New subsection 32B(1) includes the criteria for the Attorney-General to authorise an application, including that a Tribunal has made a request in relation to access to data held in a computer, that the Attorney-General is satisfied that a proceeding is before, or an investigation is being conducted by, the Tribunal and that the Tribunal has given appropriate undertakings on use of data, destruction of information and any other matters that the Attorney-General thinks appropriate.

714. New subsection 32B(2) and (3) clarify the scope and meaning of terms used in subsection (1).

715. The amendment enables Australian authorities to use the new computer access warrant powers to obtain information on behalf of a Tribunal established under the *International War Crimes Tribunals Act 1995* pursuant to a request. This is consistent with the approach taken to requests for mutual legal assistance from foreign countries as set out in new section 15CC of the MACMA.

716. The threshold requirements of the SD Act will apply when an application is made.

717. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*. That Act inserts provisions that enable assistance to be provided to war crimes tribunals that are established under the *International War Crimes Tribunals Act 1995*.

Surveillance Devices Act 2004

Item 135 - Subsection 6(1) (definition of international assistance application)

718. This item amends the definition of international assistance application under the SD Act to add reference to applications for a computer access warrant made under an international assistance authorisation.

719. The *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018* inserts a definition of international assistance application into the SD Act, and provides processes for assistance to the International Criminal Court and war crimes tribunals in relation to surveillance device warrants.

720. The amendment allows an international assistance application relating to new computer access warrants to be made in relation to the new category of international assistance to the International Criminal Court and war crimes tribunals, consistently with the approach taken for mutual legal assistance.

721. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 136 - Subsection 6(1) (paragraph (a) of the definition of *international assistance authorisation*)

722. This item adds new section 15CC(1) of the MACMA to the definition of international assistance authorisation under the SD Act.

723. The *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2017* inserts a definition of *international assistance authorisation* into the SD Act, and provides processes for assistance to the International Criminal Court and war crimes tribunals in relation to surveillance device warrants.

724. New section 15CC(1) allows the Attorney-General to authorise requests by foreign countries for assistance in relation to data held in computers under new computer access warrant provisions.

725. The amendment allows an international assistance authorisation relating to new computer access warrants to be made in relation to the new category of international assistance to the International Criminal Court and war crimes tribunals, consistently with the approach taken for mutual legal assistance.

726. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 137 - Subsection 27A(4)

727. This item replaces subsection 27A(4) to refer to 'international assistance authorisations' instead of 'mutual assistance authorisations.'

728. New section 27A allows law enforcement to apply for a computer access warrant in specified circumstances, including in relation to an international assistance authorisation.

729. This amendment is consequential to reflect the new definition of international assistance authorisation in item 136.

730. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 138 - Paragraphs 27C(1)(c) and (2)(a)

731. This item removes the reference to 'mutual assistance authorisation' and replaces it with 'international assistance authorisation'.

732. New section 27C deals with the determination of applications for computer access warrants, including specific criteria for decision-making in the case of a warrant sought in relation to an international assistance authorisation under paragraph 27C(1)(c) and (2)(a).

733. This amendment is consequential to reflect the new definition of international assistance authorisation in item 136.

734. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 139 - Paragraph 27C(2)(f)

735. This item replaces proposed new paragraph 27C(2)(f) to reflect the new definition of international assistance authorisations under item 136.

736. New section 27C deals with the determination of applications for new computer access warrants, including mandatory considerations for the issuing authority in the case of a warrant sought in relation to an international assistance authorisation.

737. This amendment is consequential to reflect the new definition of international assistance authorisation in item 136.

738. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 140 - Subparagraph 27D(1)(b)(iv)

739. This item removes the reference to 'mutual assistance authorisation' and replaces it with 'international assistance authorisation'.

740. New section 27D provides for what a computer access warrant must contain, including where the warrant relates to an international assistance authorisation.

741. This amendment is consequential to reflect the new definition of international assistance authorisation in item 136.

742. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 141 - Paragraph 27E(3)(c)

743. This item removes the reference to 'mutual assistance authorisation' and replaces it with 'international assistance authorisation'.

744. New section 27D provides for what a computer access warrant authorises, including when data is covered by a warrant in the case of a warrant sought in relation to an international assistance authorisation.

745. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 142 - Paragraph 27H(4)(a)

746. This item removes the reference to 'mutual assistance authorisation' and replaces it with 'international assistance authorisation'.

747. New section 27H deals with discontinuance of access under a computer access warrant, including obligations for the chief officer to take steps to ensure access is

discontinued in circumstances where the warrant has been sought by or on behalf of a law enforcement officer as authorised under an international assistance authorisation.

748. This amendment is consequential to reflect the new definition of international assistance authorisation in item 136.

749. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 143 - Subparagraph 27H(4)(b)(i)

750. This item removes the reference to offences against a law of a foreign country in the proposed paragraph.

751. New section 27H deals with discontinuance of access under warrant. Section 27H requires the chief officer to take steps to ensure access is discontinued including where the chief officer of the law enforcement agency is satisfied that access to data under the warrant is no longer required for the purpose of enabling evidence to be obtained of the commission of the offence against a law of a foreign country to which the authorisation relates.

752. This amendment is consequential to reflect the new definition of international assistance authorisation in item 136. It reflects that the jurisdiction of the International Criminal Court and war crimes tribunals may relate to crimes under international law and are not limited to crimes against the laws of a particular country.

753. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 144 - Paragraph 27H(9)(c)

754. This item removes the reference to ‘mutual assistance authorisation’ and replaces it with ‘international assistance authorisation’.

755. This item also removes the reference to ‘offence against a law of a foreign country to which an authorisation relates’ and replaces it with ‘any offence to which the authorisation relates.’

756. New section 27H deals with discontinuance of access under warrant, including obligations on a law enforcement officer where they believe that access to data under the warrant is no longer necessary for the purposes in relation to an international assistance authorisation.

757. This amendment is consequential to reflect the new definition of international assistance authorisation in item 136. It reflects that the jurisdiction of the International Criminal Court and war crimes tribunals may relate to crimes under international law and are not limited to crimes against the laws of a particular country.

758. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 145 - Subsection 64A(4)

759. This item removes the reference to ‘mutual assistance authorisation’ and replaces it with ‘international assistance authorisation’.

760. New section 64A allows for assistance orders to be made requiring a person with knowledge of a computer or a computer system to assist access, including in the case of a computer that is the subject of a computer access warrant issued in relation to an international assistance authorisation.

761. This amendment is consequential to reflect the new definition of international assistance authorisation in item 136.

762. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Item 146 - Application of amendments

763. This item sets out the application of the contingent amendments contained in Schedule 2, Part 3.

764. The amendments would apply a request made to the Attorney-General by the International Criminal Court, a Tribunal or a foreign country on commencement of the item.

765. It would also have retrospective application to a request that is made before commencement of the item if, immediately before that commencement, the Attorney-General had yet to make a decision on the request.

766. The amendments would apply to requests whether conduct, a crime or an offence to which the request relates occurred before, on or after commencement.

767. Commencement of this item is subject to commencement of the *Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018*.

Schedule 3 – Search warrants under the *Crimes Act 1914*

Item 1 – Subsection 3C(1)

768. This item inserts definitions of *account-based data*, *carrier*, *communication in transit*, *electronic service* and *telecommunications facility* into the Crimes Act.

769. Account-based data is detailed at item 2 of this schedule.

770. Carrier, communication in transit and telecommunications facility draw their meaning from the Telecommunications Act.

771. Electronic service has the same meaning as in *Enhancing Online Safety Act 2015*.

Item 2 – After section 3C

772. This item inserts new section 3CAA, which defines *account-based data*.

773. The purpose of including this definition is to ensure that accessing a computer or data storage device under warrant permits the executing officer or a constable assisting to use that computer or data storage device – or any other equipment – for the purpose of obtaining access to account-based data.

774. Account-based data in relation to a person includes data associated with an account for an electronic service with end-users that is held by the person. This could be data associated with an email service, a Facebook account, an Instagram account, a Reddit subscription, a Twitter profile, a log-in to a commentary section on a news website or messaging services such as WhatsApp, Signal, and Telegram.

775. A person is taken to hold an account with the electronic service if they use, pay or manage an account, whether or not the account is in a particular name of a person or whether a person actually created the account. A person who inherits an account, establishes an account in a false name, shares an account, has an account established in their name, or attempts to anonymise an account, is still taken to hold the account

776. The definition of account-based data in relation to a person is not limited to the person who holds an account.

777. Account-based data in relation to a person also includes data associated with an account for an electronic service with end-users that is used or is likely to be used be the person. This could include data associated with an account held by another person (such as a family member, friend or business associate) but utilised by the first-mentioned person.

778. Account is defined in section 4 of the *Enhancing Online Safety Act 2015*. It includes a free account, a pre-paid account and anything that may reasonably be regarded as the equivalent of an account.

Item 3 – After subsection 3F(2)

779. This item inserts new subsections 3F(2A) and (2B) to make additions to the list of things authorised by a warrant issued under section 3E of the Crimes Act. The amendments

provide that the executing officer or a constable assisting may use a computer or device found during the search, a telecommunications facility, other electronic equipment or a data storage device at any time when the warrant is in force. These activities must be for the purpose of obtaining access to relevant data (subsection 3F(2A)) or account-based data (subsection 3F(2B)) in order to determine whether the data is evidential material. The executing officer or constable assisting may copy, delete or alter data if necessary to achieve this purpose.

780. Relevant data is defined in the Crimes Act and is distinguishable from account-based data by being stored within the computer or data storage device. Account-based data may be held on the device or within another computer such as an external server or cloud.

781. This amendment will allow an officer or constable assisting to utilise specialist equipment to analyse computers and digital equipment.

782. Subsection 3F(2C) provides that subsections (2A) and (2B) do not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more things specified in the warrant. In no circumstances is it authorised for material loss or damage to be caused to other persons lawfully using a computer.

783. Subsections 3F(2D) and (2E) clarify that an officer or constable assisting may access data in accordance with this section remotely. Often the remote access of devices is best practice. Notification of access is always required.

Item 4 – Subsection 3K(3A)

784. This item extends the time in which a computer or data storage device may be moved to another place for analysis from 14 days to 30 days. Things that are not computers or data storage devices will continue to be subject to the 14 day time limit for analysis.

785. The time it takes to process data has increased as technology has advanced and computers have become more complex. The extended time limit will allow proper forensic processes to be undertaken.

786. Computers and data storage devices may include any items that compute or retain data.

787. Examples of a computer include a mobile telephone, laptop, tablet and smart watch. For clarity, where a computer forms a part of a greater whole, it is permissible to relocate and examine the greater whole rather than remove the computer. For example, often vehicles contain computers. For forensic best practice, the entire vehicle may be relocated and examined rather than removing particular elements. This avoids potential damage to systems and devices.

788. Data storage devices include any things that contain or are designed to contain data for use by a computer. Data storage devices are not required to have a computational component. They are also not required to be powered. Examples of a data storage device include a CD, SD Card, USB or any other thing that contains information that is made

legible, accessible or usable by a computer. This includes future storage solutions not yet envisioned.

Item 5 – Subsection 3K(3B)

789. This item amends subsection 3K(3B) to reflect the amendment of subsection 3K(3A), that is that computers and data storage devices may be relocated for examination or analysis for a period longer than items not computers or data storage devices.

Item 6 – Subsection 3K(3D)

790. This item amends subsection 3K(3D) to reflect the amendment of subsection 3K(3A), that is that computers and data storage devices require a greater period of time for examination than other items. This subsection thus extends the maximum time period for a single extension of the original 30 day time period from seven days to 14 days for computers and data storage devices.

At the end of section 3K

791. Once a computer or data storage device is moved for processing, new subsections 3K(5) and (6) allow examination to occur by using the computer or device, a telecommunications facility, any other electronic equipment or a data storage device. These activities must be for the purpose of obtaining access to relevant data (subsection 3K(5)) or account-based data (subsection 3K(6)) in order to determine whether the computer or device is a thing that may be seized. Data may be copied, deleted or altered if necessary to achieve this purpose.

792. Subsection 3K(7) provides that subsections (5) and (6) do not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more things specified in the warrant. In no circumstances is it authorised for material loss or damage to be caused to other persons lawfully using a computer.

793. Subsections 3K(8) and (9) clarify that processing of a computer or data storage device in accordance with this section may occur remotely. Often the remote access of devices is best practice.

Item 7 – Subsection 3LAA(1)

794. This item amends subsection 3LAA(1) to accommodate the new concept of account-based data. If electronic equipment is moved to another place under subsection 3K(2), the executing officer or a constable assisting may operate the equipment to access data, data held at another place and account-based data.

Item 8 – After subparagraph 3LA(1)(a)(i)

795. New subparagraph 3LA(1)(a)(ia) allows a constable to apply to a magistrate requiring a specified person to provide information or assistance that is reasonably necessary to access data held in a computer or device found during a search of a person that is authorised by a warrant under section 3E.

796. This amendment reflects the portability of modern computers and data storage devices, including mobile telephones and USBs

Item 9 – Subsection 3LA(5)

797. This item bifurcates the existing offence in section 3LA into a simple offence and an aggravated offence.

798. The simple offence remains the same as the previous offence in section 3LA, but increases the penalty from two years imprisonment or 120 penalty units to five years imprisonment or 300 penalty units, or both.

799. The intention of raising the penalty for the simple offence is to reflect the significant harm to investigations and prosecutions caused by a person failing to assist law enforcement access computers and data storage devices covered by an order issued under section 3LA.

800. The aggravated offence applies where a person omits to do an act and the offence to which the relevant warrant relates is a serious offence or a serious terrorism offence as defined in the Crimes Act. The penalty for the aggravated offence is 10 years imprisonment or 600 penalty units, or both.

801. The new aggravated offence reflects the gravity of non-compliance with an investigation into a serious offence. Given the current penalties for committing an offence against section 3LA, there is no incentive for a person to comply with an order if they have committed an offence with a higher penalty and evidence is available on their device.

Item 10 – After paragraph 3N(2)(a)

802. This item accommodates amendments to remote access to data, including account data. The new paragraph ensures that information accessed at a place other than the premises is not subject to subsection 3N(1) where information accessed at the warrant place would be exempted under paragraph 3N(2)(a). The intent is to provide that powers introduced in this amendment are available to law enforcement at the same level of accessibility and functionality as existing powers.

Item 11 – After subsection 3ZQV(3)

803. New subsection 3ZQV(3) prohibits electronic equipment that has been seized from being operated to determine whether data generated after the expiry of the warrant is evidential material.

Item 12 – Application of amendments

804. All amendments made under the provisions of this schedule apply only to warrants and orders issued after the commencement, being the day after the Bill receives the Royal Assent.

Schedule 4 – Search warrants issued under the *Customs Act 1901*

Item 1 – Subsection 183UA(1)

805. *Communication in transit* has the same meaning as in the Telecommunications Act.

806. *Recently used conveyance* in relation to a search of a person means a conveyance that the person had operated or occupied at any time within the 24 hours before the search commenced. Search warrants issued in new section 199A, pertaining to a person, include searching recently used conveyances.

Item 1A – Subsection 183UA(1) (definition of search warrant)

807. This item amends the definition of *search warrant* to include new person-based search warrants in section 199A for the purposes of the Customs Act.

Item 2 – Subsection 183UA(1)

808. This item amends subsection 183UA(1) to include a definition of serious offence that is the same as in Part IAA of the Crimes Act. This definition is included to enable the creation of an aggravated offence for not complying with an order made under section 201A of the Customs Act. The definition of serious offence will encapsulate certain offences in the Customs Act, including:

a. Division 1AA – Export of goods for a military end-use

b. Section 50(7) – Prohibited imports licencing (narcotics)

c. Section 112(2BC) – Prohibited exports licencing (narcotics)

d. Section 64ADA – Disclosure of cargo reports to port authorities, and

e. Section 233 and associated sections – Smuggling and unlawful importation and exportation / dealing in UN sanctioned goods.

809. This definition is included to enable the creation of an aggravated offence for not complying with an order made under section 201A of the Customs Act. The intention of this amendment is not to permit the ABF to investigate serious crimes under the Crimes Act, but to include a provision that triggers serious crimes in the Customs Act.

Item 3 – Section 198 (heading)

810. This item amends the heading of section 198 so as to differentiate it from the new section 199A.

Item 4 – Section 199 (heading)

811. This item amends the heading of section 199 so as to differentiate it from the new section 199B.

Item 4A – After subsection 199(4)

812. New subsection 199(4A) make additions to the list of things authorised by a search warrant relating to a premises. The amendments provide that the executing officer or a constable assisting may use a computer or device found during the search, a telecommunications facility, other electronic equipment or a data storage device at any time when the warrant is in force. These activities must be for the purpose of obtaining access to relevant data in order to determine whether the data is evidential material. The executing officer or constable assisting may copy, delete or alter data if necessary to achieve this purpose.

813. This amendment will allow an officer or constable assisting to utilise specialist equipment to analyse computers and digital equipment.

814. Subsection 199(4B) provides that subsection (4A) does not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more things specified in the warrant. In no circumstances is it authorised for material loss or damage to be caused to other persons lawfully using a computer.

815. Subsection 199(4C) clarifies that an officer or constable assisting may access data in accordance with this section remotely. Often the remote access of devices is best practice. Notification of access is always required.

Item 5 – After section 199

816. This item inserts new section 199A and new section 199B. These sections provide for limited search warrants to be issued in regards to a person.

817. These search warrants are limited to an ordinary search or frisk search for a computer or data storage device. These search warrants are not a general search warrant power relating to persons. This power is necessary to account for the large amount of evidentiary material that is now held on or accessible by computers and data storage devices.

818. The ABF has existing powers to apply for a search warrant in regards to premises. Premises-based warrants are more permissive in that they allow ordinary searches and frisk searches of any persons on the premises. The new, limited, person-based search warrants provide a more proportionate response option for the ABF, allowing them to execute a targeted warrant when that is all that is required. For example, locations which are usually subject to premises-based search warrants – including businesses, warehouses and transport locations – are often populated and broadly-used.

819. A person may also operate multiple businesses in separate locations. Rather than applying for a premises-based warrant for each business premises, this amendment will allow the ABF to seek a warrant to search the computer or data storage device for that person.

820. The ABF has standing powers in relation to things in customs control, being items in a customs place such as a port or airport. These provisions are not intended to read down those powers.

821. Reference in paragraph 199B(1)(c) to prohibited goods that are 'unlawfully carried by the person' draws the definition of prohibited goods from the Customs Act. Reference to seizable items draws the definition from the Customs Act. The intention of this provision is to ensure that an officer executing a search authorised under section 199A may seize items that are clearly and illegitimately in the possession of the person being searched. This could include narcotics, firearms or other prohibited goods. This would also extend to any recently used conveyance, should prohibited goods or seizable items be found.

822. It is not the intention of paragraph 199(1)(c) to provide a backdoor means for officers to search persons for such prohibited goods or seizable items. The intention of the warrant is to obtain evidentiary material found in a computer or data storage device. Only goods found incidental to this search may be seized. Searches primarily for goods other than computers and data storage devices should be conducted under a section 198 search warrant for a premises, a section 203 seizure warrant or another provision available to ABF officers. The section 199A search warrant is not a general, broad-based search warrant.

823. Dealing with items seized under section 199A is not amended by this legislation.

824. For clarity, provisions in paragraph 199B(1)(c) regarding prohibited goods unlawfully carried, require an executing officer or person assisting to form a reasonable belief that the goods are prohibited goods and that they are carried unlawfully. It is reasonable for an executing officer or person assisting to assume that prohibited goods are not carried lawfully, given their nature, i.e. an amount of marijuana is by its objective nature an illicit substance, and does not require a subjective assessment. It would be unreasonable for an executing officer or person assisting to assume that prohibited goods are lawfully carried, barring some demonstration of material indicating otherwise. The onus is on the person subject to a search and seizure to provide material demonstrating that prohibited goods are carried lawfully, such as a prescription, import licence or firearms licence. If material demonstrating the goods were lawfully carried can be provided following seizure, those goods may be returned subject to provisions in sections 203R and 203S of the Customs Act. Should the goods already be delivered to the custody of the AFP, the provisions relating to seizure of goods under the Crimes Act would apply to those goods rather than provisions in the Customs Act. The person concerned must also deal with the AFP directly regarding the return of the goods. The ABF is not required to act as an intermediary in these circumstances.

825. A search warrant issued in respect of a person, that under section 199B permits a search of a recently used conveyance, also allows lawful entry to that recently used conveyance. This is consistent with the Crimes Act.

Item 5A – Subsection 200(1)

826. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 5AA – Subsection 200(2)

827. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 5B – Paragraph 200(2)(b)

828. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 5C – Paragraph 200(3)(a)

829. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 5D - Paragraph 200(3)(b)

830. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 6 – Subsection 200(3A)

831. This item extends the period for which a computer or data storage device can be moved for examination to determine whether it contains or constitutes evidentiary material to 30 days. The current 72 hour period is inadequate to account for many of the internal authorisation and relocation processes which must occur to ensure transparency and accountability, as well as secure relocation of devices once moved. This results in few items of potential evidential value being moved for analysis.

832. The 72 hour period is also inadequate for proper forensic processes to be undertaken, even where relocation and approval occurs within the timeframe. The time it takes to process data has increased as technology has advanced and computers have become more complex. To ensure forensic best-practice for computers and data storage devices, an adequate time period is necessary.

833. Subsection 200(3A) applies to computers or data storage devices relocated or examined under section 198 or section 199A of the Customs Act. That is, the new subsection applies to items obtained from a person based or premises-based search warrant.

834. Examples of a computer include a mobile telephone, laptop, tablet, smart watch. For clarity, where a computer forms a part of a greater whole, it is permissible to relocate and examine the greater whole rather than remove the computer. For example, often vehicles contain computers. For forensic best practice, the entire vehicle may be relocated and examined rather than removing particular elements. This avoids potential damage to systems and devices.

835. Data storage devices include any things that contain or are designed to contain data for use by a computer. Data storage devices are not required to have a computational component. They are also not required to be powered. Examples of a data storage device include a CD, SD card, USB or any other thing that contains information that is made legible, accessible or usable by a computer. This includes future storage solutions not yet envisioned.

Item 7 – Subsection 200(3B)

836. This item amends subsection 200(3B) for consistency with amendments made to subsection 200(3A) in item 2 of this schedule.

Item 7A – Subsection 200 (3C)

837. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 8 – After subsection 200(3C)

838. This item aligns the timeframes for extension for relocating and examining computers and data storage devices to the extended timeframes in the Crimes Act. This provision will allow a maximum extension of 14 days for computers and data storage devices.

Item 8AA - Subsection 200(4)

839. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 8A - After section 201

840. This item replicates provisions in the Crimes Act, and those in the Customs Act related to existing premises based warrants, to allow the use of electronic equipment moved under other provisions (the person based search warrant inserted by this schedule) to access data on that electronic equipment, and for related purposes.

841. If evidentiary material is found on the item, it may be seized.

Item 9 – Paragraphs 201A(1)(a), (b) and (c)

842. This item allows orders in section 201A to be made against person-based or premises-based search warrants. Section 201A is amended to apply when a computer or data storage device has been found in the course of executing a warrant under section 198 or section 199A, or apply to any computer or data storage device seized under the Subdivision.

Item 10 – Paragraph 201A(2)(a)

843. For completeness, reference to data storage devices is included to enable searches of those devices.

Item 11 – Subparagraph 201A(2)(b)(ii)

844. For completeness, reference to data storage devices is included to enable searches of those devices.

Item 12 – Subparagraph 201A(2)(b)(iii)

845. For completeness, reference to data storage devices is included to enable searches of those devices.

Item 13 – At the end of paragraph 201A(2)(b)

846. This item inserts three additional categories of persons who can be compelled to provide assistance with accessing a device under order. These definitions are consistent with

those in the Crimes Act. The intention is to ensure that powers are consistent, and that powers are fully effective by including all such persons that could reasonably be expected to provide assistance with accessing a device under an order.

Item 14 – Subparagraph 201A(2)(c)(i)

847. For completeness, reference to data storage devices is included to enable searches of those devices.

Item 15 – Subparagraph 201A(2)(c)(i)

848. For completeness, reference to data storage devices is included to enable searches of those devices.

Item 16 – Subparagraph 201A(2)(c)(i)

849. This item clarifies that computers or data storage devices that have been removed from a network may be the object of an assistance order.

Item 17 – Subparagraph 201A(2)(c)(ii)

850. For completeness, reference to data storage devices is included to enable searches of those devices.

Item 18 – Subsection 201A(3)

851. This item bifurcates the existing offence in section 201A into a simple offence and an aggravated offence.

852. The simple offence remains the same as the previous offence in section 201A, but increases the penalty from two years imprisonment or 120 penalty units to five years imprisonment or 300 penalty units, or both.

853. The intention of raising the penalty for the simple offence is to reflect the significant harm to investigations and prosecutions caused by a person failing to assist law enforcement access computers and data storage devices covered by an order issued under section 201A.

854. The aggravated offence applies where a person omits to do an act and the offence to which the relevant warrant relates is a serious offence or a serious terrorism offence as defined in the Crimes Act. The penalty for the aggravated offence is 10 years imprisonment or 600 penalty units, or both.

855. The new aggravated offence reflects the gravity of non-compliance with an investigation into a serious offence. Given the current penalties for committing an offence against section 201A, there is no incentive for a person to comply with an order if they have committed an offence with a higher penalty and evidence is available on their device.

Item 18A - Paragraph 201B(1)(a)

856. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 18B - Paragraph 201B(1)(d)

857. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 18C - Paragraph 202(1)(a)

858. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 18D - Paragraph 202A(2)(a)

859. This item is a consequential amendment, differentiating between existing premises based search warrants and the new, limited, person based search warrant.

Item 19 – Subsection 203K(5)

860. This item adds a reference to the new subsection 199A(1) into subsection 203K(5). Section 203K relates to 'special powers available to executing officers'.

Item 20 – Subsection 203M(4)

861. This item adds a reference to the new section 199A into subsection 203M(4). Section 203M relates to 'warrants by telephone or other electronic means'.

Item 21 – Application of amendments

862. All amendments made under the provisions of this Schedule apply only to warrants and orders issued after the commencement, being the day after the Bill receives the Royal Assent.

Schedule 5 – Australian Security Intelligence Organisation

Part 1 – *Australian Security Intelligence Organisation Act 1979*

Item 1 – After subsection 16(1)

863. This item provides that the Director-General may, by writing, delegate any or all of his or her functions or powers under the new section 21A, Voluntary assistance provided to the Organisation, to a senior position-holder of ASIO, which is defined in the ASIO Act as an SES employee or equivalent, or a Coordinator.

864. The intention is that the default position in paragraph 34AB(1)(b) of the *Acts Interpretation Act 1901* applies, that is the powers that may be delegated do not include that power to delegate. Due to the sensitivity of the decisions being made (decisions to request assistance or issue evidentiary certificates), it is appropriate that this power be confined to SES employees or equivalent and not be sub-delegated.

Item 2 – At the end of Division 1 of Part III

865. This item adds a new section 21A regarding the provision of voluntary assistance to ASIO. Section 21A establishes two frameworks which provide protection from civil liability for voluntary assistance provided in accordance with a Director-General request and for unsolicited disclosure of information.

866. Subsection 21A(1) provides that if the Director-General requests a person or body to engage in conduct that the Director-General is satisfied is likely to assist ASIO in the performance of its functions and:

a. the person engages in the conduct in accordance with the request, and

b. the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory, and

c. the conduct does not result in significant loss of, or serious damage to, property

the person or body is not subject to any civil liability for, or in relation to, that conduct. The requirement for the Director-General to be satisfied that the conduct is likely to assist ASIO in the performance of its functions is intended to provide greater legal certainty to recipients of requests, by allowing them to rely on the Director-General's satisfaction.

867. A request by the Director-General may be made orally or in writing. If a request is made orally then the Director-General must make a written record of the request within 48 hours of it being made.

868. This item also provides that the Director-General may enter into a contract, agreement or arrangement with a person or body in relation to conduct engaged in by the person or body in accordance with such a request.

869. This item also provides protection from civil liability for persons or bodies making unsolicited disclosures of information to ASIO. The amendment provides that if a person or

body engages in conduct that consists of, or is connected with giving information to ASIO, or giving or producing a document to ASIO, or making one or more copies of a document and giving those copies to ASIO, and:

a. the person reasonably believes that the conduct is likely to assist ASIO in the performance of its functions, and

b. the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory, and

c. the conduct does not result in significant loss of, or serious damage to, property, and

d. a Director-General request discussed above does not apply to the conduct

the person or body is not subject to any civil liability for, or in relation to, the conduct.

870. Given this amendment relates to unsolicited help, the policy intention is to ensure that someone who reasonably believes that their help will assist benefits from the immunity, even if they are mistaken about what may assist ASIO, or what the ASIO's functions are.

871. This item also provides that ASIO may make and retain copies of, or take and retain extracts from, a document given or produced to ASIO in accordance with a Director-General request or an unsolicited disclosure of information.

872. This item also provides that the Director-General may give a certificate in writing certifying one or more facts relevant to the question of whether he or she was satisfied that particular conduct was likely to assist ASIO in the performance of its functions.

873. In any proceedings that involve determining whether the provisions relating to a Director-General request or unsolicited disclosure of information applies to particular conduct, a certificate given by the Director-General is prima facie evidence of the facts certified. The evidentiary certificate would only deal with factual matters, being the factual basis on which the Director-General reached his or her belief, and would not deal with legal matters that would be properly the role of the courts to determine.

874. In the event that the operation of this section results in an acquisition of property, within the meaning of paragraph 51(xxxi) of the Constitution, from a person otherwise than on just terms, this item provides that the Commonwealth is liable to pay a reasonable amount of compensation to the person. If the Commonwealth and the person do not agree on the amount of compensation, the person may institute proceedings in the Federal Court of Australia for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.

Item 3 – Section 23

Item 4 – At the end of Division 2 of Part III

875. This item inserts a new subdivision concerning assistance relating to access to data. Given the inherent challenges ASIO faces due to encryption, there is a pressing requirement for ASIO to be able to gain access to data stored on computer devices and networks in an unencrypted form in order to better understand the national security threat environment.

876. New 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 one or more of the following:

(a) access data held in, or accessible from, a computer or data storage device that:

- is the subject of a warrant under section 25A, 26 or 27A; or
- is the subject of an authorisation under section 27E or 27F; or
- is on premises in relation to which warrant under section 25, 26 or 27A is in force; or
- is on premises in relation to which an authorisation under section 27D or 27F is in force; or
- is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by warrant under section 25 or 27A; or
- is found in the course of an ordinary search of a person, or a frisk search of a person, authorised under section 27D; or
- has been removed from premises under a warrant under section 25, 26 or 27A; or
- has been removed from premises under section 27D; or
- has been seized under section 34ZB;

877. The types of assistance that ASIO may seek under this power include compelling a target or a target's associate to provide the password, pin code, sequence or fingerprint necessary to unlock a phone subject to a section 25 computer access warrant. Another example is where a specialist employee of a premise subject to a section 25 search warrant could assist ASIO officers interrogate the relevant electronic database or use the relevant software so that they can obtain a copy of particular records or files.

(b) copy data held in, or accessible from, a computer, or data storage device, described in paragraph (a) to another data storage device;

(c) convert into documentary form or another form intelligible to an ASIO employee or ASIO affiliate:

- data held in, or accessible from, a computer, or data storage device, described in paragraph (a) above; or
- data held in a data storage device to which the data was copied as described in paragraph (b); or
- data held in a computer or data storage device removed form premises under a warrant under section 25, 26 or 27A; or

- data held in a computer or data storage device removed from premises under section 27D.

878. The Attorney-General can make the order if the Attorney-General is satisfied that:

(a) if the computer or data storage device:

- is the subject of a warrant under section 27A; or
- is on premises in relation to which a warrant under section 27A is in force; or
- is found in the course of an ordinary search of a person, or a frisk search of a person, authorised by a warrant under section 27A; or
- has been removed from premises under a warrant under section 27A;

both:

- access by ASIO to data held in, or accessible from, the computer or data storage device will be for the purpose of obtaining foreign intelligence relating to a matter specified in the relevant notice under subsection 27A(1); and
- on the basis of advice received from the Defence Minister or the Foreign Affairs Minister, the collection of foreign intelligence relating to that matter is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being; and

(b) if paragraph (a) does not apply – there are reasonable grounds for suspecting that access by ASIO to data held in, or accessible from, the computer or data storage device will substantially assist the collection of intelligence in accordance with this Act in respect of a matter that is important in relation to security; and

(c) the specified person is:

- reasonably suspected of being involved in activities that are prejudicial to security; or
- the owner or lessee of the computer or device; or
- an employee of the owner or lessee of the computer or device; or
- a person engaged under a contract for services by the owner or lessee of the computer or device; or
- a person who uses or has used the computer or device; or
- a person who is or was a system administrator for the system including the computer or device; and

(d) the specified person has relevant knowledge of:

- the computer or device or a computer network of which the computer or device forms or formed a part; or

- measures applied to protect data held in, or accessible from, the computer or device.

879. This power enables ASIO to compel those who are able to provide ASIO with knowledge or assistance on how to access to data on computer networks and devices to do so. Similar powers are available to the police under section 3LA of the Crimes Act which allows a constable to apply to a magistrate for an order requiring a specified person with knowledge of a computer or a computer system to assist in accessing data on a computer or data storage device.

880. Where the computer or data storage device is not on premises in relation to which a warrant is in force, the order must: specify the period within which the person must provide the information or assistance; and specify the place at which the person must provide the information or assistance; and specify the conditions (if any) determined by the Attorney-General as the conditions to which the requirement on the person to provide the information or assistance is subject.

881. This item provides that a person commits an offence if the person is subject to an order under this section; and the person is capable of complying with the order; and the person omits to do an act; and the omission contravenes the order. A person would be incapable of complying with an order where, for example, the person was in possession of information, documents or things but the information, document or thing had been removed from their possession, or deleted or destroyed by another person. The penalty is imprisonment for 5 years or 300 penalty units, or both.