2016

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

# COUNTER-TERRORISM LEGISLATION AMENDMENT BILL (NO. 1) 2016

EXPLANATORY MEMORANDUM

(Circulated by authority of the

Attorney-General, Senator the Honourable George Brandis QC)

## COUNTER-TERRORISM LEGISLATION AMENDMENT BILL (NO. 1) 2016

## GENERAL OUTLINE

1. The Counter-Terrorism Legislation Amendment Bill (No. 1) 2016 (the Bill) replaces the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 (the 2015 Bill) and includes provisions implementing recommendations contained in the February 2016 advisory report of the Parliamentary Joint Committee on Intelligence and Security (the Committee) on the 2015 Bill (the Committee advisory report), and recommendations made by the Independent National Security Legislation Monitor (INSLM) in his February 2016 *Report on the impact on journalists of section 35P of the ASIO Act* (INSLM report).

2. The Bill contains a package of amendments to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), *Administrative Appeals Tribunal Act 1975* (AAT Act), *Classification (Publications, Films and Computer Games) Act 1995* (Classification Act), *Criminal Code Act 1995* (*Criminal Code*), *Crimes Act 1914* (Crimes Act), *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act), *Public Interest Disclosure Act 2014* (PID Act), *Taxation Administration Act 1953* (TA Act), *Telecommunications (Interception and Access) Act 1979* (TIA Act), and *Surveillance Devices Act 2004* (SD Act).

3. These measures are being developed in response to lessons from recent counter-terrorism operations and represent part of the Government's comprehensive reform agenda to strengthen Australia's national security and counter-terrorism legislation.

## FINANCIAL IMPACT STATEMENT

4. The measures in the Bill have little financial impact on Government expenditure or revenue.

## STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

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

### Counter-Terrorism Legislation Amendment Bill (No. 1) 2016

5. The Counter-Terrorism Legislation Amendment Bill (No. 1) 2016 (the 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

#### *Administrative Appeals Tribunal Act 1975*

6. The Bill amends section 40 of the ASIO Act, requiring consequential technical amendments to the AAT Act.

#### *Australian Security Intelligence Organisation Act 1979*

7. Currently, the Australian Security Intelligence Organisation (ASIO) can only furnish a security assessment either directly to a state or territory in respect of a designated special event or in all other cases indirectly via a Commonwealth agency. Such arrangements are resource intensive and significantly hinder the timely provision of security assessments to state and territory authorities. The Bill amends the ASIO Act to enable ASIO to furnish security assessments directly to states and territories.

8. The Bill also makes amendments to implement recommendations contained in the INSLM report. These amendments will introduce new protections to the section 35P regime requiring that disclosure of information made by members of the community, except those who received the relevant information in their capacity as an entrusted person, will only constitute an offence if the information will endanger the health or safety of a person or prejudice the effective conduct of a special intelligence operation (SIO). The amendments will also include a defence of prior publication available only to persons who did not receive the relevant information in their capacity as an entrusted person.

#### *Classification (Publications, Films and Computer Games) Act 1995*

9. Under the Classification Act, a publication, film or computer game that directly or indirectly advocates a terrorist act is classified Refused Classification (RC) and cannot be published in Australia. Currently, 'advocates' means 'counsels' or 'urges'. The Bill amends the Classification Act to bring the meaning of 'advocates the doing of a terrorist act' into line with the revised definition in the *Criminal Code* by also including the expressions 'promotes' and 'encourages'.

#### *Crimes Act 1914*

10. There are impediments to monitoring a person's compliance with a control order imposed by an issuing court on the person. That is because search warrants with an investigatory purpose can only be issued where there is information demonstrating an offence is currently occurring or has already occurred. The Bill amends the Crimes Act to establish a new regime for monitoring the compliance of individuals subject to a control order through

monitoring search warrants – not to gather evidence of the commission of a crime that has already occurred. The Bill establishes complementary regimes for monitoring compliance with control orders under the TIA Act and SD Act. The regimes include important safeguards including the threshold for issuing warrants, ministerial and other reporting requirements, and independent oversight by the Commonwealth Ombudsman.

11. When the delayed notification search warrant regime was inserted into the Crimes Act in 2014, the threshold for issue required not only the applicant (eligible officer), but also the police officer approving the application (chief officer) and the person considering whether to approve the warrant (eligible issuing officer) to suspect and believe certain things on reasonable grounds. The Bill amends the delayed notification search warrant regime to clarify that while the eligible officer must suspect and believe those matters on reasonable grounds, the chief officer and eligible issuing officer are not required to personally hold the relevant suspicions and belief. Rather, they must be satisfied that there are reasonable grounds for the eligible officer to hold those suspicions and belief.

***Criminal Code Act 1995***

12. Australia continues to face a serious terrorist threat. This heightened threat environment has seen an increased operational tempo from Australia's law enforcement agencies to protect the public from terrorist acts, including some widely noted counter-terrorism operations conducted by Joint Counter-Terrorism Teams comprising the Australian Federal Police (AFP), state police, ASIO officers and members from other relevant agencies. The amendments to the *Criminal Code* would further strengthen and enhance our existing laws, provide additional safeguards and limitations, and implement outstanding recommendations of independent reviews of our laws, including by:

- creating a new offence prohibiting conduct advocating genocide in Division 80 (Treason, urging violence and advocating terrorism or genocide)
- removing the authority of the Family Court of Australia and judges of the Family Court of Australia to issue control orders and preventative detention orders (PDOs)
- ensuring that receiving funds for providing legal assistance as to whether an organisation is a 'terrorist organisation' is not criminalised
- authorising an issuing court to impose a control order on persons 14 years and older, and providing appropriate safeguards
- ensuring that a person subject to a requirement to wear a tracking device under a control order is also required to maintain the tracking device in good operational order, and
- clarifying the test for the issuing of a PDO.

***National Security Information (Criminal and Civil Proceedings) Act 2004***

13. The amendments to the NSI Act include:

- enhancing the ability to protect national security information in control order proceedings

- incorporating a role for a special advocate to represent the interests of the subject of a control order proceeding when the subject and their legal representative have been excluded from hearing or seeing sensitive national security information
- allowing a court to make an order that is inconsistent with regulations made under the NSI Act if the Attorney-General has applied for the order, and
- ensuring the regulations continue to apply where an order is made under sections 22 or 38B (Arrangements for federal criminal proceedings / for civil proceedings about disclosures etc. of national security information) to the extent that the regulations relate to issues not included in the order.

***Surveillance Devices Act 2004***

14. As noted above, there are impediments to monitoring a person's compliance with a control order imposed by an issuing court on the person because SD warrants generally have an investigatory purpose. The amendments to the SD Act establish a new regime for monitoring the compliance of individuals subject to a control order through surveillance device warrants. The Bill establishes complementary regimes for monitoring compliance with control orders under the Crimes Act and TIA Act. The regimes include important safeguards including the threshold for issuing warrants, ministerial and other reporting requirements, and independent oversight by the Commonwealth Ombudsman.

15. Amendments to the SD Act will enable law enforcement agencies to deal with protected information in connection with control order and PDO proceedings nationally, in line with the AFP's existing ability to use information obtained under the TIA Act in Commonwealth PDO proceedings.

***Public Interest Disclosure Act 2014***

16. The Bill amends section 8 of the PID Act to include orders made under revised section 38J of the NSI Act (in Part 1 of Schedule 15 of the Bill) within the definition of 'designated publication restriction'.

***Taxation Administration Act 1953***

17. The TA Act prohibits taxation officers from recording or disclosing protected information unless one of the listed exceptions is satisfied. The amendments would create an additional exception to the offence provision, authorising taxation officers to record or disclose information to an Australian government agency for the purposes of preventing, detecting, disrupting or investigating conduct related to a matter of security as defined in the ASIO Act. The amendments also authorise agencies that receive such information to further disclose that information to the Commonwealth Ombudsman. These amendments implement Recommendation 20 of the Committee advisory report.

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

18. As noted above, there are impediments to monitoring a person's compliance with a control order imposed by an issuing court on the person because TI warrants generally have an investigatory purpose. The amendments to the TIA Act establish a new regime for monitoring the compliance of individuals the subject of a control order through telecommunications interception warrants. The Bill establishes complementary regimes for

monitoring compliance with control orders under the Crimes Act and SD Act. The regimes include important safeguards including the threshold for issuing warrants, ministerial and other reporting requirements, and independent oversight by the Commonwealth Ombudsman.

19. Amendments to the TIA Act will separately enable law enforcement agencies to use lawfully intercepted information in connection with control order and PDO proceedings nationally, in line with the AFP's existing ability to use such information in Commonwealth PDO proceedings.

**Human Rights Implications**

**Amendments that do not engage human rights**

***Administrative Appeals Tribunal Act 1975***

20. The amendments to the AAT Act are technical amendments and consequential to the amendments made by the Bill to section 40 of the ASIO Act. They do not engage any human rights.

***Australian Security Intelligence Organisation Act 1979***

**Provision of security assessments directly to states and territories**

21. The Bill amends section 40 (Assessments for State purposes) of the ASIO Act to enable ASIO to furnish security assessments directly to a state or territory or an authority of a state or territory in circumstances in which any prescribed administrative action in respect of a person by the state, territory or authority could affect security. Currently, ASIO can only provide a security assessment to a state via a Commonwealth agency (except in the case of a designated special event) which severely hinders the timely provision of security assessments to state authorities.

22. 'Security assessment' and 'prescribed administrative action' are defined in section 35 and 'security' in section 4.

23. Minor changes will be made to the provisions providing for the rights of notice and review to ensure they extend to assessments provided directly to a state or territory or an authority of a state or territory. For example, the subject of an adverse security assessment provided to a state can seek review of the assessment from the Administrative Appeals Tribunal (AAT). Section 61 (Effect of findings) of the ASIO Act provides that the AAT findings, to the extent that they do not confirm the assessment, supersede that assessment. The Bill amends section 61 to clarify that a state or a state authority must also treat such AAT findings as superseding the assessment.

24. As this amendment is designed to streamline an existing process, it does not raise any particular human rights concerns.

*Crimes Act 1914*

**Delayed notification search warrants**

25. Amendments to Part IAAA (Delayed notification search warrants) of the Crimes Act clarify the suspicion and belief requirements for the issue of a delayed notification search warrant (DNSW). An AFP officer applying for a DNSW must suspect on reasonable grounds that offences have been, are being, are about to be or are likely to be committed and that entry and search of the premises will substantially assist in the prevention or investigation of one or more of those offences. The officer must on reasonable grounds believe that it is necessary for the entry and search to be conducted without the knowledge of the occupier of the premises or anyone present at the premises.

26. The AFP Commissioner, who must authorise the AFP officer to apply for a DNSW, and the eligible issuing officer (a judge of the Federal Court of Australia or of a state or territory Supreme Court or a nominated AAT member) need only be satisfied that there are reasonable grounds for the AFP officer to hold that suspicion and belief. They do not need to personally hold the suspicion and belief and would not usually be in a position to form that suspicion and belief. The amendments clarify that the Commissioner and eligible issuing officer must be independently satisfied that the AFP officer does hold the requisite suspicion and belief and that there are reasonable grounds for holding them.

27. While the DNSW regime has privacy implications, the amendments themselves clarify what was intended under the Crimes Act and do not raise particular human rights concerns.

*Criminal Code Act 1995*

**Removal of the Family Court of Australia as an issuing authority for control orders and continued preventative detention orders**

28. Courts that may issue control orders pursuant to Division 104 (Control orders) are currently defined in section 100.1 (Definitions) as the Federal Court of Australia, the Family Court of Australia and the Federal Circuit Court of Australia. Amending section 100.1 to remove reference to the Family Court and authorise only the Federal Court and the Federal Circuit Court to issue control orders partly implements a recommendation of the Council of Australian Governments (COAG) 2013 Review that the Federal Court should be the only issuing court. COAG agreed with the review panel that the Family Court is a specialist court and that the control orders function fits more appropriately with the broad general federal law jurisdiction exercised by the Federal Court and Federal Circuit Court which are more familiar with the types of powers and functions required to administer the regime.

29. Section 105.2 (Issuing authorities for continued preventative detention orders) sets out who may be appointed as an issuing authority for continued PDOs, including serving and retired judges of the Family Court of Australia or of a State. Amendments to sections 100.1 (Definitions) and 105.2 remove the ability for serving and retired judges of the Family Court to be appointed as issuing authorities for the purpose of issuing continued PDOs. These amendments ensure that only judges who have served in a court which ordinarily exercises functions relevant to criminal law and counter-terrorism will be eligible for appointment as an issuing authority for PDOs.

30. These amendments do not have any human rights implications.

**Getting funds to, from or for a terrorist organisation**

31. The amendments to subsection 102.6(3) expand the existing exemption to an offence under section 102.6 so that it is not an offence to receive funds for the sole purpose of providing legal advice in connection with the question of whether the organisation is a terrorist organisation.

32. The amendment provides greater scope for the receipt of funds from an organisation and does not raise any human rights concerns.

***Public Interest Disclosure Act 2014***

33. The amendment to the PID Act arises from the amendments to the NSI Act contained in Part 1 of Schedule 15 of the Bill. The amendment to the PID Act ensures that the new orders under revised section 38J of the NSI Act are included in the definition of 'designated publication restriction', which already includes orders made under existing sections 31 and 38L of the NSI Act.

34. The amendment does not have any human rights implications.

**Human rights implications**

35. The Bill engages the following human rights:

- the right to an effective remedy in Article 2 of the *International Covenant on Civil and Political Rights* (ICCPR)
- the right to life in Article 6 of the ICCPR
- the right to liberty and security of the person and to freedom from arbitrary arrest or detention in Article 9 of the ICCPR
- the right to freedom of movement in Article 12 of the ICCPR
- the right to a fair trial, the right to minimum guarantees in criminal proceedings and in a suit at law and the presumption of innocence in Article 14 of the ICCPR
- the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR
- the right to freedom of expression in Article 19 of the ICCPR
- the prohibition on advocacy of racial or religious hatred in Article 20 of the ICCPR (noting Australia has a reservation in relation to this Article)
- the right to freedom of association in Article 22 of the ICCPR
- the rights of parents and children in Articles 23 and 24 of the ICCPR
- the prohibition on cruel, inhuman or degrading treatment or punishment in Article 7 of the ICCPR and the *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (CAT) (particularly Article 16)

- the right of the child to have their best interests as a primary consideration by courts of law, administrative authorities or legislative bodies in Article 3 of the *Convention on the Rights of the Child* (CRC)
- the right of the child not to be separated from their parents against their will, unless this is in the best interests of the child, in Article 9 of the CRC
- the right of the child to freedom of expression in Article 13 of the CRC
- the right of the child to freedom of thought, conscience and religion in Article 14 of the CRC
- the right of the child to freedom of association in Article 15 of the CRC, and
- the right to protection against arbitrary and unlawful interferences with privacy in Article 16 of the CRC.

***Australian Security Intelligence Organisation Act 1979***

**Unauthorised disclosure of information**

*Right to a fair trial – Article 14(1) of the ICCPR, right to freedom from arbitrary detention – Article 9 of ICCPR, the prohibition on cruel, inhuman or degrading treatment or punishment in Article 7 of ICCPR and the CAT and right to freedom of movement – Article 12 of ICCPR*

36. Article 9 of the ICCPR provides that no-one shall be subjected to arbitrary arrest or detention or deprived of their liberty except on such grounds and in accordance with such procedure as are established by law. The UN Human Rights Committee has stated that 'arbitrariness' includes the elements of inappropriateness, injustice and a lack of predictability. An arrest or detention must be reasonable and necessary in all circumstances with reference to the recurrence of crime, interference with evidence or the prevention of flight.

37. Article 12 of the ICCPR provides that everyone lawfully within the territory of a State shall, within the territory, have the right to liberty of movement. This right can be permissibly limited if the limitations are provided by law, are necessary to protect national security or the rights and freedoms of others and is consistent with the other rights in the ICCPR.

38. Article 14(1) of the ICCPR provides that in the determination of obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.

39. Article 7 of the ICCPR and the CAT prohibit conduct which may be regarded as cruel, inhuman or degrading treatment or punishment ('ill treatment') and can be either physical or mental. The UN treaty bodies responsible for overseeing the implementation of these treaties have provided guidance on the sort of treatment that is prohibited. Examples of cruel, inhuman or degrading treatment include unduly prolonged detention that causes mental harm. Punishment may be regarded as degrading if, for instance, it entails a degree of humiliation beyond the level usually involved in punishment. These rights are absolute and cannot be limited in any way.

40. The Bill engages the rights to a fair trial, freedom from arbitrary detention, protection from cruel, inhuman or degrading treatment or punishment and freedom of movement on the basis that it creates new offences in section 35P with maximum penalties of five and ten years imprisonment.

41. Although the Bill contains four new offences to replace the two existing offences in section 35P, its effect is to increase the burden on the prosecution in relation to 'outsider' offences. The Bill retains the existing offences for ASIO insiders, and introduces additional elements that must be proven before an 'outsider' can be convicted of an offence.

42. Existing section 35P contains two offences for the unauthorised disclosure of information relating to an SIO, which apply regardless of whether or not a person holds a position of trust in relation to ASIO information. The basic offence applies when the person is reckless as to whether the information disclosed relates to an SIO. The aggravated offence applies when the person also intended to endanger the health or safety of any person or prejudice the effective conduct of an SIO, or the person knows that disclosure will endanger the health or safety of any person or prejudice the effective conduct of an SIO. Following the INSLM report, section 35P has been amended to create separate offences for 'insiders' (persons who came to the knowledge or into the possession of relevant information in their capacity as an entrusted person) and 'outsiders' (persons to whom the information came to their knowledge or into their possession other than in the person's capacity as an entrusted person). While this results in an increased number of offences, this simply reflects the fact that outsiders will be subject to separate offences and will no longer be held to the same, stricter, standard as ASIO insiders.

43. The insiders offences are identical to those in existing section 35P. The basic offence contains no harm requirement, and the aggravated offence applies where a person intends to cause harm, or the disclosure will in fact cause harm.

44. For the new 'outsider' offences, the basic offence will contain an additional harm requirement. The basic offence will require the person to be reckless as to whether the disclosure will endanger a person's health or safety, or compromise the effective conduct of an SIO. A person will not commit an offence if the information they disclose is completely harmless. The aggravated offence will require either knowledge or intention in relation to the harm. This is consistent with the INSLM's recommendations and reflects the higher standard of conduct that insiders should be held to in relation to their use, handling and disclosure of sensitive information.

45. Penalties of five and ten years imprisonment are not so significant that they would constitute arbitrary detention or cruel, inhuman or degrading treatment or punishment, or an unlawful restriction on the freedom of movement. Persons participating in an SIO do so on explicit and strict conditions that are additional to any other obligations applying to an ASIO affiliate or employee, and they are potentially subject to greater risks should information pertaining to an SIO be disclosed. The penalties implement a gradation consistent with established principles of Commonwealth criminal law policy, as documented in the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers. The Guide provides that a heavier maximum penalty is appropriate where the consequences of an offence are particularly dangerous or damaging.

46. The maximum penalty of five years imprisonment applying to each basic offence and the maximum penalty of ten years imprisonment for each aggravated offence reflects an

appropriate gradation. These penalties reflect an appropriate gradation with offences relating to unauthorised dealing in sections 18A and 18B, which carry a maximum 3 year penalty. The unauthorised disclosure of information regarding an SIO is considered more culpable than the unauthorised dealing with information pertaining to ASIO's statutory functions.

47. The penalty of up to ten years imprisonment applying to the aggravated offence maintains parity with the penalty applying to the offence of unauthorised communication in section 18 of the ASIO Act. The heavier penalty is appropriate considering the greater level of harm, with the aggravated offence requiring either the intention to jeopardise a person's safety or prejudice the effective conduct of an SIO, or the actual compromise of a person's safety or prejudice to the SIO.

*Freedom of expression – Article 19 of ICCPR*

48. Article 19(2) of the ICCPR provides that everyone has the right to freedom of expression, including the freedom to impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media. Article 19(3) provides that this right may be limited on grounds including national security. However, any limitations must be prescribed by legislation and be reasonable, necessary and proportionate to achieve the desired purpose.

49. The Bill engages the right to freedom of expression through making it an offence to disclose information relating to an SIO. This is critical as the very nature of an SIO is covert. Communicating such sensitive information can place the health and safety of participants at risk. It also negates the integrity of operations in general and affects the conduct of the operation in question, hindering ASIO's ability to counter threats to national security, including threats of terrorism. As such, the limitation on the right is necessary for both the protection of national security and the health and safety of participants.

50. The offences are reasonable as they distinguish between entrusted persons and outsiders, provide appropriate defences and retain important safeguards facilitating the operation of oversight and accountability bodies. The offences in subsections 35P(1) and (1B) apply a higher standard to a person who receives information in their capacity as an entrusted person, which reflects the greater culpability and existence of a duty of confidence that applies to those who receive information relating to an SIO in their official capacity. The offences applying to outsiders in new section 35P(2) and (2A) will include a harm requirement, so that journalists and other third parties who report on information that will not endanger the health or safety of a person or prejudice the conduct of an SIO will not be guilty of an offence. The offences in new section 35P reflect a reasonable limitation on the right to freedom of expression, adjusted according to whether the person is an entrusted person or an outsider.

51. A new defence will also be included to cover disclosure of information that is already in the public domain. New subsection 35P(3A) provides a defence, only available to individuals who did not receive the relevant information in their capacity as an entrusted person, where the relevant information has already been made publicly available. This provides an exception to the offence and demonstrates that the offence limits the freedom of expression no more than is reasonable and necessary.

52. SIOs remain subject to oversight and accountability mechanisms, which are maintained by section 35P. For example, pursuant to subsection 18(9) of the IGIS Act, the offence would not apply to a document that was dealt with for the purpose of producing information under subsection 18(1) of the IGIS Act. Further, the offence would not apply in accordance with section 10 of the PID Act if information was dealt with for the purpose of making a public interest disclosure in accordance with the PID Act as it applies to ASIO. For example, a person could report a matter in relation to an SIO to the IGIS.

***Classification (Publications, Films and Computer Games) Act 1995***

**Definition of 'advocates the doing of a terrorist act'**

53. Paragraph 9A(2)(a) (Refused Classification for publications, films or computer games that advocate terrorist acts) of the Classification Act is amended to give 'advocates the doing of a terrorist act' the same meaning as that given under paragraph 102.1(1A)(a) of the *Criminal Code*. This ensures that a publication, film or computer game that directly or indirectly 'promotes' or 'encourages' (as well as 'counsels' or 'urges') the doing of a terrorist act must be classified Refused Classification (RC), so cannot therefore be published under state and territory classification enforcement laws.

*The right to freedom of expression in Article 19 of the ICCPR, the prohibition on advocacy of racial or religious hatred in Article 20 of the ICCPR*

54. Article 19(2) of the ICCPR provides that everyone has the right to freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds through any media. However, Article 19(3) provides that the freedom of expression may be limited where the limitations are provided for by law and are necessary for the protection of national security. This restriction on free expression is justified on the basis that advocating the commission of a terrorist act or terrorism offence is conduct which jeopardises the security of Australia, the personal safety of its population and its national security interests.

55. Article 20(2) sets out a requirement for laws to prohibit any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

56. Terrorist acts represent the gravest threats to the welfare of Australians as they include causing serious physical harm or death, damaging property, creating a serious risk to the health or safety of the public and interfering with electronic systems. It is reasonable that such conduct should not be advocated and that reasonable steps should be taken to discourage behaviour that promotes such actions. Importantly, deterring the advocacy of such acts promotes the rights of others (in accordance with Article 19(3)(a)). In this instance, this may include protecting people's right to life as covered by Article 6 of the ICCPR.

57. This restriction on freedom of expression is a reasonable, necessary and proportionate measure to protect the public from terrorist acts. Individuals who travel overseas to participate in foreign conflicts often return with radicalised ideologies that include violent extremism. Advocating terrorism heightens the probability of the commission of terrorism offences on Australian soil and encourages others to join the fight overseas.

58. The RC classification for material that 'promotes' or 'encourages' (as well as 'counsels' or 'urges') the doing of a terrorist act does not disproportionately limit freedom of expression. Material that is classified RC contains content that is very high in impact and

falls outside generally accepted community standards, including the category of detailed instruction or promotion in matters of crime or violence.

59. Accordingly, the limitation on the freedom of expression is reasonable, necessary and proportionate and unlikely to be greater than the restriction as it is currently worded. Article 20(2) also supports the expanded definition of advocating a terrorist act and the prohibition of such advocacy.

***Crimes Act 1914***

**Monitoring warrants for control orders**

60. Division 104 of Part 5.3 of the *Criminal Code* currently provides for a range of obligations, prohibitions and restrictions (controls) to be imposed on a person to prevent terrorism and hostile activities overseas. The Crimes Act and other Commonwealth legislation confer a range of investigatory powers on law enforcement and other agencies, including the search warrant regime in Division 2 of Part IAA of the Crimes Act. However, Australian law does not provide adequate powers for law enforcement agencies to monitor compliance with controls under a control order to sufficiently reduce the risk that a person will engage in terrorist act planning or preparatory acts while subject to a control order.

61. The former INSLM noted in his 2012 Annual Report that the efficacy of a control order depends largely upon the subject's willingness to respect a court order, and that in the absence of the ability to effectively monitor a person's compliance with the terms of a control order, there is no guarantee that a person will not breach the order or go on to commit a terrorist offence. This is a position shared by our law enforcement agencies. That is because existing Commonwealth coercive powers in relation to the conduct of physical searches, telecommunication interception and surveillance devices are only available for the purposes of investigating an offence that has already been committed or is about to be committed.

62. The amendments create a 'monitoring warrant' regime in a new Part IAAB of the Crimes Act which applies to individuals subject to control orders. Unlike the existing search warrant regime, the new regime will not require the issuing authority to be satisfied that an offence has already occurred or is going to be committed.

63. If warrants were only available once law enforcement had a suspicion that an offence had already occurred, a controlee might already have been able to provide support for terrorist activity or take preparatory steps for a terrorist act. If a person were able to perform these kinds of actions before law enforcement agencies could take action, the preventative and protective purposes of control orders would be undermined. Consequently, this regime adopts a threshold appropriate to the monitoring of a person in relation to whom a superior court has already decided the relevant threshold for issue of a control order has been met and who therefore, by definition, is of security concern.

64. It is imperative that our law enforcement agencies have adequate powers to monitor a person's compliance with the conditions of the control order. Without sufficient powers to monitor compliance, community safety may be put at risk if the person does not choose to comply with the conditions of the order and breaches go undetected. Furthermore, the knowledge that law enforcement is able to use its powers to actively monitor compliance with a control order provides a strong disincentive to a person to breach the conditions of a control order. This enhances the effectiveness of the control order regime.

65. The regime is modelled on the monitoring regime in the *Regulatory Powers (Standard Provisions) Act 2014* (RPSP Act) and the existing search warrant provisions in the Crimes Act. The SD Act and the TIA Act are also being amended by this Bill to confer powers on law enforcement agencies to monitor compliance with control orders.

66. Where a search is to be conducted of the premises or vehicle owned or occupied by or in the possession of the person who is subject to a control order, entry can be either under a warrant or by consent of the person (provided the person has authority to give consent). Consistent with section 25 of the RPSP Act, the AFP must notify the person subject to the control order that they can refuse consent. The person can also withdraw consent.

67. The monitoring powers in sections 19 and 20 of the RPSP Act are reproduced in the regime, including searching premises; inspecting, examining, measuring or testing things on the premises; inspecting or copying documents; and operating electronic equipment to put data into documentary form or to transfer data to a disk, tape or other storage device. The powers under section 24 of the RPSP Act to ask the occupier to answer questions and produce any document relevant to compliance with the conditions of the control order are also reproduced.

68. The new regime also imports section 17 of the RPSP Act, which ensures that, even where a monitoring warrant is in place, the person has the right not to answer questions or produce documents if the answers or documents might tend to incriminate them or if they can claim legal professional privilege. The new regime provides that before a constable asks or requires a person to answer a question or produce a document they must explain to the person their rights concerning legal professional privilege and privilege against self-incrimination. Further, the regime provides that should a constable fail to explain to the person their rights in relation to answering a question or producing a document any answer given or document produced will not be admissible as evidence against the person in a criminal proceeding. These amendments implement Recommendation 10 of the Committee advisory report.

69. Before issuing a monitoring warrant the issuing officer is under a positive obligation to consider whether the exercise of monitoring powers under the warrant would be likely to have the least interference with the liberty and privacy of any person that is necessary in all of the circumstances. This requirement implements Recommendation 9 of the Committee advisory report, and is intended to achieve an appropriate balance between the objectives of the regime to mitigate risks and protect the community, and the privacy of individuals.

70. The monitoring warrant regime incorporates important reporting requirements and independent oversight by the Commonwealth Ombudsman regarding the operation of the regime.

*The right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR*

71. Article 17 of the ICCPR provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.

72. Lawful interference with the right to privacy is permitted under Article 17 of the ICCPR, provided it is not arbitrary. In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be for a reason consistent with the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights

Committee has interpreted the requirement of 'reasonableness' to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances.

73. Entry to and search of a person's home by consent will engage, but will not limit, the protection from arbitrary and unlawful interference with privacy in Article 17. The person will not be compelled to answer questions or produce documents when requested by police. Entry and search are only authorised if consent is informed and voluntary, limiting the impact on privacy.

74. Entry to and search of a person's home under a monitoring warrant (and without consent) will engage, and limit, the protection from arbitrary and unlawful interference with privacy in Article 17. The person is compelled to answer questions and produce documents as required by police unless doing so might tend to incriminate them or if they can claim legal professional privilege. Entry and search under a monitoring warrant affects the person's privacy.

75. Although third parties present at premises may be questioned regardless of whether the premises are entered on the basis of consent or a premises monitoring warrant, they are under no obligation to provide information or documents unless a monitoring warrant in relation to premises is in force. Accordingly, even where a warrant is in force, questioning or requests for documents can only occur where the purpose relates to one or more of the four prescribed purposes set out in paragraphs 3ZZKE(3)(c)-(f).

76. Further safeguards are also built into the regime where entry and search is under a monitoring warrant. They include a requirement that the monitoring warrant issuing officer is satisfied on the balance or probabilities that, where a search is to be conducted of the premises or vehicle owned or occupied by or in the possession of the person who is the subject of a control order, the search is reasonably necessary and reasonably appropriate and adapted to the purposes of:

- protecting the public from a terrorist act
- preventing the provision of support for, or the facilitation of, a terrorist act
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or
- determining whether the relevant control order has been, or is being, complied with.

77. Similarly, surveillance devices or the interception of telecommunications will only be available where they would be likely to substantially assist in one of these four purposes listed above.

78. Furthermore, the regime imposes a positive obligation on an issuing officer to have regard to whether allowing one or more constables to exercise the monitoring warrant powers would be likely to have the least interference with any person's liberty and privacy that is necessary in the circumstances. This requirement acknowledges the infringement of these powers on a person's privacy by striking an appropriate balance between the objectives of the regime in mitigating risk and protecting the public, against the right to privacy of the subject of the control order.

79. The Crimes Act regime is closely modelled on the existing provisions in the RPSP Act, which sets out a range of powers relevant to monitoring, investigation and

enforcement purposes. The powers in relation to entry and inspection by consent are consistent with those in the RPSP Act. The powers in relation to seizure of potential evidence—which can only be exercised under a monitoring warrant, not where entry was by consent—are modelled on the existing search warrant regime in Part IAA of the Crimes Act.

80. The interference with the right to privacy is proportionate and limited to ensuring that a person who is subject to a control order is prevented from engaging in any activity related to terrorist acts and terrorism offences. The monitoring warrant powers are subject to appropriate limitations which ensure that the use of power is reasonable and necessary. These measures require the monitoring warrant issuing officer to be satisfied of thresholds that mean that the powers cannot be used in an arbitrary fashion and that the level of intrusiveness is no more than necessary to achieve a legitimate objective. This legitimate objective is to assist law enforcement officers to prevent serious threats to community safety. The potentially intrusive nature of the powers is balanced by their use solely in respect of terrorism offences, which constitute the gravest threat to the safety of Australians.

81. The new regime protects against arbitrary abuses of power as the entry, monitoring, search and information gathering powers are conditional upon consent by the occupier of the premises, with seizure only possible by prior judicial authorisation. Where entry is based on the occupier's consent, the consent must be informed and voluntary and the occupier can restrict entry for a particular period. Authorised persons and any persons assisting them must leave the premises if the occupier withdraws consent.

82. The new regime specifies that an issuing officer of a warrant to enter premises for the purpose of monitoring must be a judicial officer. In addition, an authorised person cannot enter premises unless their identity card is shown to the occupier of the premises. If entry is authorised by warrant, the authorised person must also provide a copy of the warrant to the occupier. This provides for the transparent use of the relevant powers and mitigates arbitrariness and the risk of abuse.

83. The regime includes a number of other safeguards and accountability mechanisms, record keeping and reporting requirements, and independent oversight by the Commonwealth Ombudsman. These features implement Recommendation 11 of the Committee advisory report. The regime provides that the AFP Commissioner must keep a record of each monitoring warrant issued, each instrument revoking a monitoring warrant and any order granting an extension to a monitoring warrant period. The AFP Commissioner must also notify the Commonwealth Ombudsman that a warrant has been issued, provide a copy of the warrant and notify the Ombudsman of any contravention of a provision of Part IAAB by an AFP member. Furthermore, the Ombudsman must report annually to the Attorney-General on the compliance of members of the AFP with Part IAAB. The Attorney-General must report to the Parliament on the operation of the regime, including the number of warrants issued and executed and must also include, in full, the Ombudsman's report on the AFP's compliance with the regime.

84. The monitoring warrant powers 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, a number of important protections are built into the regime to ensure any interference is reasonable, necessary and proportionate to achieve a legitimate objective—the effective operation of control orders for the purpose of maintaining community safety. Safeguards and limitations on the use of regulatory powers ensure that such lawful interferences with a person's privacy are not arbitrary or at risk of abuse.

*Criminal Code Act 1995*

**New offence of advocating genocide**

85. Division 80 of the *Criminal Code* (Treason, urging violence and advocating terrorism) currently contains a range of offences for urging or advocating certain conduct, including terrorism, which attracts a maximum penalty of seven years imprisonment.

86. Division 268 (Genocide, crimes against humanity, war crimes and crimes against the administration of the justice of the International Criminal Court) sets out the offences concerning genocide carried out by various means. All attract a penalty of life imprisonment. In section 80.2D of the renamed Division 80 (Treason, urging violence and advocating terrorism or genocide), the Bill creates the new offence of advocating the commission of any of the genocide offences in sections 268.3 to 268.7.

87. The new offence is modelled on the recently enacted offence prohibiting advocating terrorism in section 80.2C of the *Criminal Code*, but has some important differences that reflect the relevant international instruments.

88. The meaning of 'advocates' in section 80.2D is consistent with that in subsection 80.2C(3), that is, to 'counsel, promote, encourage or urge' genocide. The new offence provides that a person commits an offence if the person engages in conduct reckless as to whether another person will engage in genocide. The new offence also reflects subsection 80.2C(4), which provides that advocating genocide is an offence, even if the genocide itself does not occur.

89. The offence applies to advocacy of genocide of people who are outside Australia or the genocide of national, ethnic, racial or religious groups in Australia and the advocacy itself can occur either in Australia or overseas.

90. Subsection 80.2D(2) provides a double jeopardy protection, which states that a person cannot be tried by a federal court or a state or territory court for an offence against subsection 80.4D(1) if the person has already been convicted or acquitted by the International Criminal Court for an offence constituted by substantially the same conduct.

91. The maximum penalty for advocating genocide will be seven years imprisonment. This reflects that the conduct is at least as serious as advocating terrorism, but less serious than inciting genocide under section 11.4 and Division 268, which requires that the offender would have to 'intend' that genocide occur, and carries a maximum penalty of ten years imprisonment.

*The right to freedom of expression in Article 19 of the ICCPR and the prohibition on advocacy of racial or religious hatred in Article 20 of the ICCPR*

92. Article 19(2) of the ICCPR provides that everyone has the right to freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds through any media. However, Article 19(3) provides that the exercise of this freedom carries special duties and responsibilities and may therefore be limited where the limitations are provided for by law and are necessary for respect of the rights or reputations of others.

93. It is reasonable that genocide should not be advocated and that reasonable steps should be taken to discourage behaviour that promotes such activity. Importantly, deterring

the advocacy of genocide promotes the rights of others (in accordance with Article 19(3)(a)). In this instance, this may include protecting people's right to life as covered by Article 6 of the ICCPR.

94. Article 20(2) sets out a requirement for laws to prohibit any advocacy for national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. This also supports the provision of an offence of advocating genocide as discrimination, hostility and violence may all be drivers of genocide.

95. Australia however entered the following reservation to Article 20 when ratifying the ICCPR:

- Australia interprets the rights provided by Articles 19 [freedom of opinion and expression], 21 [right of peaceful assembly] and 22 [freedom of association] as consistent with Article 20; accordingly the Commonwealth and the constituent States, having legislated with respect to the subject matter of the Article in matters of practical concern in the interests of public order (*ordre public*), the right is reserved not to introduce any further legislative provision on these matters.

96. Australia regards the requirement for prohibition by law provided for in Article 20(2) as consistent with the right to freedom of opinion and expression in Article 19. The United Nations Human Rights Committee has noted that the acts addressed in Article 20 are all subject to restriction pursuant to Article 19(3), which allows for the freedom of opinion and expression to be subject to restrictions to ensure respect for the rights or reputations of others and for the protection of national security, public order, public health or morals.

97. While the reservation suggests Australia does not believe that it must do more to meet its obligation under Article 20 as existing laws already fulfil that obligation, it does not prevent Australia from creating further offences if a need were identified.

98. A person charged with the offence of advocating genocide may be able to rely on the good faith defences in section 80.3, which protect freedom of expression in certain circumstances, including in relation to artistic works, public discussion or debate, and news and current affairs. This strengthens the view that the new offence is not out of step with Article 19 and would only target conduct that is unjustifiable and that poses a substantial risk to particular groups of people.

99. This restriction on freedom of expression is a reasonable, necessary and proportionate measure to protect particular groups of people from the threat of genocide, whether in Australia or overseas. Accordingly, a limitation on the freedom of expression in this case is reasonable, necessary and proportionate.

*The punishment of certain acts in relation to genocide, including direct and public incitement to commit genocide, in Articles III and IV of the Genocide Convention*

100. This amendment bolsters Australia's commitment to implementing its obligations under the Convention on the Prevention and Punishment of the Crime of Genocide (Genocide Convention). Article III states that genocide, conspiracy to commit genocide, direct and public incitement to commit genocide, attempt to commit genocide and complicity in genocide are punishable acts. Article IV states that persons committing genocide or any of the other acts enumerated in Article III shall be punished, whether they are constitutionally

responsible rulers, public officials or private individuals. The amendment more fully addresses the 'direct and public incitement to commit genocide' in Article III by ensuring that public advocacy of the forms of genocide reflected in sections 268.3 to 268.7 of the *Criminal Code* are punishable, even without any of the genocide-related acts actually having been carried out.

101. It should be noted that the Genocide Convention, unlike the ICCPR, is not one of Australia's seven 'core' conventions against which the human rights compatibility of legislation must be measured. Australia is also not seeking to extend its jurisdiction to cover acts of genocide carried out overseas. Its human rights obligations are primarily confined to Australian territory.

**Reduction in minimum age for control orders**

102. Control orders under Division 104 of Part 5.3 of the *Criminal Code* have been a tool available to law enforcement since 2005.

103. Control orders are a protective mechanism and constitute an important element of the counter-terrorism strategy. They provide the AFP with a means to request that a court impose obligations, prohibitions and restrictions (controls) on a person for the purpose of protecting the public from a terrorist act. Law enforcement may have sufficient information or intelligence to establish serious concern regarding the threat posed by an individual, but may not have sufficient time or evidence to lay charges and commence a criminal prosecution. In these circumstances, control orders provide a mechanism to manage the threat in the short to medium term. Use of a control order is therefore considered in conjunction with, and is complementary to, criminal prosecution, and allows a balance to be achieved between mitigating the risk to community safety and allowing criminal investigations to continue.

104. The control order regime has been used judiciously to date. This reflects the policy intent that these orders are not punitive in nature and do not act as a substitute for criminal proceedings. Rather, they should only be invoked in limited circumstances and are subject to numerous legislative safeguards that preserve the fundamental human rights of a person subject to a control order.

105. Control orders can currently be made only in relation to persons 16 years of age or older. Subsection 104.28(1) (Special rules for young people) specifically prevents a control order being requested, made or confirmed in relation to a person who is under 16 years of age. Further, special safeguards apply to control orders made in relation to a person aged 16 or 17 years. Specifically, a control order can only be made for a maximum duration of three months, rather than the maximum of 12 months applicable for persons over 18 years of age.

106. Section 104.28(1) builds upon the existing control order regime to allow a control order to be requested, made or confirmed in respect of a young person who is 14 or 15 years of age. The amendment will expand the control order regime to children from 14 years of age, and will apply the existing safeguards and additional safeguards on such control orders. This age threshold is higher than the age at which a child can be prosecuted for a criminal offence in Australia (ten years of age).

107. The lowering of the minimum age follows incidents, both in Australia and overseas, organised or led by young persons below 16 years of age. With school-age students being

radicalised and engaging in radicalising others and capable of participating in activity which poses a threat to national security, the age limit of 16 years is no longer sufficient if control orders are to be effective in preventing terrorist activity.

108. The vulnerability of young people to violent extremism demands proportionate, targeted measures to divert them from extremist behaviour. It is appropriate and important that all possible measures are available to avoid a young person engaging with the formal criminal justice system and to mitigate the threat posed by violent extremism. Consequently, the ability to use control orders to influence a person's movements and associations, thereby reducing the risk of future terrorist activity, addresses a substantial concern and the regime is aimed and targeted at achieving a legitimate objective.

109. It should be noted that control orders are not a punitive measure but a preventative and protective measure. They are intended, as stated in paragraph 104.4(1)(d), to protect the public from a terrorist act, to prevent the provision of support for the facilitation of a terrorist act, or to prevent support for or the facilitation of engagement in a hostile activity in a foreign country.

110. A control order does not authorise detention. A young person will not be separated from family and will be able to attend school. Where the issuing court is satisfied on the balance of probabilities that a restriction on the young person's movements is reasonably necessary and appropriate and adapted to achieving one of the purposes of the control order regime, it can impose a requirement that the young person remain at specified premises between specified times each day or on specified days. This 'curfew' can be for up to a total of 12 hours in any 24-hour period.

111. The court can also require that the young person wear a tracking device, require them to be photographed and fingerprinted, and require that they report to specified people at particular times and places. They can be prohibited or restricted from being at certain places, leaving Australia, communicating with specified people or accessing particular forms of telecommunications or technology, including the internet, possessing or using of specified articles or substances and the carrying out of specified activities.

112. The penalty for contravening a control order is five years imprisonment, regardless of the age of the subject (section 104.27). Prosecution for the offence would require proof that the young person intentionally breached the relevant condition.

113. The rights discussed below are mainly those in the CRC. It should be noted that the CRC does not have an equivalent to the right to freedom of movement as set out in Article 12 of the ICCPR.

*The right of the child to have their best interests as a primary consideration by courts of law, administrative authorities or legislative bodies in Article 3 of the CRC*

114. Article 3 of the CRC requires that the best interests of the child shall be a primary consideration for all actions concerning social welfare institutions, courts of law, administrative authorities or legislative bodies.

115. Paragraph 104.4(1)(d) of the *Criminal Code* requires that before imposing a control on a person the court must be satisfied on the balance of probabilities that the control is reasonably necessary, and reasonably appropriate and adapted to protecting the public from a

terrorist act, or preventing the provision of support for or the facilitation of the engagement in, a terrorist act or engagement in a hostile activity overseas.

116. The amendments specify the matters the court must consider when determining what is 'reasonably necessary, and reasonably appropriate and adapted'. Specifically in relation to young persons, Division 104 (Control Orders) will require the issuing court to give consideration to the 'best interests' of a person who is 14 to 17 years of age. 'Best interests' is consistent with Article 3. In determining what is in their best interests, new subsection 104.4(2A) (Making an interim control order) provides that the court must take into account:

- the age, maturity, sex and background (including lifestyle, culture and traditions) of the person
- the physical and mental health of the person
- the benefit to the person of having a meaningful relationship with their family and friends
- the right of the person to receive an education
- the right of the person to practise their religion, and
- any other matter the court considers relevant.

117. This list of factors is adapted from the *Family Law Act 1975* (Family Law Act) and is consistent with Article 3 of the CRC. This will ensure that the particular circumstances and vulnerabilities of the young person are taken into account in determining their 'best interests' before a control order is issued or confirmed.

118. The Family Law Act requires the best interests of the child to be treated as 'the paramount' consideration when considering whether to make certain orders. In contrast, as recommended by the Committee, the paramount consideration with respect to control orders is the safety and security of the community. Accordingly, rather than being the paramount consideration, the issuing court will be required to consider the young person's best interests as a primary consideration. New subsection 104.4(2A) treats the young person's best interests as 'a primary' consideration.

119. For all control orders, regardless of the person's age, the court must take into account, as an 'additional consideration', the impact of each control on the person's circumstances, including their financial and personal circumstances (subsection 104.4(2)).

120. As is the case now for persons who are 16 to 17 years of age, control orders for all those who are 14 to 17 years of age will be for a maximum of three months from the day on which the interim order was made (subsection 104.28(2)), although this does not prevent the court from making successive orders (subsection 104.28(3)).

121. Reasonable steps must also be taken to serve the interim control order, variations of the control order, a revocation of the control order and confirmation of the interim control order on at least one parent or guardian of the young person (paragraph 104.12A(2)(c)).

122. All potential subjects of a control order, including young persons, must be informed of their right to seek legal advice and legal representation in relation to control order proceedings (subparagraph 104.12(1)(b)(iiia)).

123. This amendment will be supplemented by practical steps designed to ensure the young person has information about how to find and access legal advice and representation. In particular, when serving the young person, the AFP will provide, in writing, contact details for the relevant legal aid service in the jurisdiction. Given a young person who has been served with a control order is likely to experience feelings of uncertainty or confusion, a document providing the details about where to go for legal assistance is expected to be the best way of ensuring the young person has the information they need when they need it. In addition, the application of existing processes and agreements would mean a young person subject to a control order would always have access to legal aid. The National Partnership Agreement on Legal Assistance Services sets priorities for the delivery of legal assistance. Under that Agreement, children and young people are a priority client group and matters where the defendant is a child are a priority service area.

124. Other rights set out in the CRC, including the right to health care (Article 24) and the right not to be separated from their parents against their will (unless separation is in the best interests of the child) (Article 9), are recognised indirectly in new subsection 104.4(2A). Subsection 104.4(2A) lists the matters a court is to take into account when determining the child's best interests. The right of the child to an education (Article 28) and to practise their religion (Articles 14 and 30) are explicitly recognised.

125. A control order would only be issued against a young person, especially one as young as 14, in the rare circumstance that it was required to prevent a young person from being involved in a terrorist act. This includes protecting a young person who may be acting under the direction or influence of an extremist group or individual. In these circumstances, the wellbeing and best interests of a young person may be adversely affected if a control order is not issued in relation to that young person. For example, the issuing of a control order in relation to a young person may prevent the young person contacting the group or individual who may be encouraging the young person to engage in terrorist-related conduct.

126. A control order would only be issued against a young person where the existing issuing criteria have been satisfied in order to protect the broader community against the threat of a terrorist act. The proposal to allow the imposition of control orders on young persons would not replace existing mechanisms such as those available under the Family Law Act to ensure young persons living in an unsafe environment have access to appropriate support.

*The right to freedom of expression in Article 13 of the CRC, the right of the child to freedom of thought, conscience and religion in Article 14 of the CRC, the right of the child to freedom of association in Article 15 of the CRC, the right to protection against arbitrary and unlawful interferences with privacy in Article 16 of the CRC, the right to freedom of movement in Article 12 of the ICCPR*

127. Any combination of the controls listed in subsection 104.5(3) may be imposed as a term of a control order:

- a prohibition or restriction on the person being at specified areas or places
- a prohibition or restriction on the person leaving Australia
- a requirement that the person remain at specified premises between specified times each day, or on specified days

- a requirement that the person wear a tracking device
- a prohibition or restriction on the person communicating or associating with specified individuals
- a prohibition or restriction on the person accessing or using specified forms of telecommunication or other technology (including the internet)
- a prohibition or restriction on the person possessing or using specified articles or substances
- a prohibition or restriction on the person carrying out specified activities (including in respect of his or her work or occupation)
- a requirement that the person report to specified persons at specified times and places
- a requirement that the person allow himself or herself to be photographed
- a requirement that the person allow impressions of his or her fingerprints to be taken
- a requirement that the person participate in specified counselling or education.

128. These conditions have at least the potential to enliven Articles 13, 14, 15 or 16 of the CRC, along with Article 12 of the ICCPR. Articles 13, 14 and 15 of the CRC and Article 12 of the ICCPR provide for exceptions which are provided by law and which are necessary to protect national security and/or public safety, public order, public health or morals, or the rights and freedoms of others. Instead of the rights and freedoms of others, Article 13 provides for laws necessary for respect for the rights or reputations of others. Article 16 of the CRC (like the equivalent Article 17 in the ICCPR) does not provide permissible exceptions.

129. Article 13 of the CRC provides that children have the right to freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, in any form or through any medium. However, Article 13 also provides that freedom of expression may be restricted if lawful and necessary, including for the protection of national security. This restriction on free expression is justified on the basis that the commission of a terrorist act or terrorism offence is conduct which jeopardises the security of Australia, the personal safety of its population and its national security interests.

130. A control order may include a prohibition or restriction on a young person's use of social media. This restriction will be justified if it is aimed at preventing the young person from using social media to support or facilitate a terrorist act.

131. Article 14—the right of the child to freedom of thought, conscience and religion—may be engaged by the prohibition or restriction on being at specified areas or places (paragraph 104.5(3)(a)) if these include places of religious worship or places where the person may seek material related to their thoughts or beliefs such as bookshops or libraries. Article 14 provides that this freedom may be subject to such limitations as are prescribed by law and are necessary to protect public safety, order, health or morals, or the fundamental rights and freedoms of others. There is therefore clear scope to limit this freedom if necessary to protect the general public.

132. The restriction on being at particular places may engage the young person's freedom of association under Article 15, along with the prohibitions on communicating or associating

with specified individuals and on carrying out specified activities, and a requirement that the young person report to specified persons at specified times and places.

133. Like Article 14, Article 15 provides that this freedom may be subject to such restrictions which are in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order, the protection of public health or morals, or the protection of the rights and freedoms of others. A control order would only impose limitations on the people a young person can associate with if doing so is in the interests of national security or public safety and the rights and freedoms of others.

134. Imposition of a tracking device is one of the controls that can be imposed by an issuing court as part of a control order. In relation to young persons aged 14 to 17 years, the issuing court would need to take into account whether it is in the young person's best interests to impose such a control, noting the visible nature of a tracking device. As with all controls, the court could only impose this requirement, including the ancillary requirements in new subsection 104.5(3A), if it were reasonably necessary, and reasonably appropriate and adapted to achieving one of the purposes set out in Division 104.

135. Imposition of a tracking device on a young person will raise issues with respect to the right not to be subjected to unlawful and arbitrary interferences with privacy in Article 16 of the CRC (in the same way that it would for an adult under Article 17 of the ICCPR). For the interference with privacy not to be 'arbitrary', the interference must be reasonable, necessary and proportionate in the particular circumstances.

136. Situations where the imposition of a tracking device on an adult may be reasonable may be assessed as not being reasonable in relation to a young person in the same circumstances. For example, an issuing authority will need to assess the extent to which a visible tracking device on their wrist or ankle is likely to affect a young person's ability to attend school and to participate effectively in school. The circumstances where it would be reasonable to impose a tracking device on a person as young as 14 are likely to be limited.

137. Photographs and impressions of fingerprints obtained under paragraphs 104.5(3)(j) and (k) are collected, stored and disclosed in accordance with both the Australian Privacy Principles and section 104.22 (Treatment of photographs and impressions of fingerprints). Section 104.22 requires that photographs or fingerprints obtained from the subject of a control order must only be used for the purpose for which they were taken—ensuring identification and enforcement of the order—and that photographs and fingerprints must be destroyed 12 months after a control order period unless proceedings in relation to the control order have not yet been brought.

138. The CRC does not have an article equivalent to Article 12 of the ICCPR which states that everyone has the right to freedom of movement within their own country and the freedom to leave any country, including their own.

139. Among the controls that may be placed on an individual—adult or young person—subject to a control order is that they may be restricted from being in specified areas or places (paragraph 104.5(3)(a)), they may be prohibited from leaving Australia (paragraph 104.5(3)(b)), and they may be required to remain at specified premises between specified times each day, or on specified days (paragraph 104.5(3)(c)). Freedom of movement can be permissibly limited under Article 12 if the limitations are provided by law

and are necessary to achieve a legitimate purpose, such as protecting national security and public order.

140. The control order regime is comprehensively prescribed by legislation. A person subject to a control order will only have their right to freedom of movement restricted on grounds clearly established by domestic law and on grounds which are in accordance with the requirements of Division 104. As well as being authorised by law, the purpose of the control order regime is to protect the Australian public from a terrorist act. This is because the circumstances in which a control order may be sought are where the issuing court is satisfied on the balance of probabilities that:

- the order would 'substantially assist in preventing a terrorist act'
- a person has been providing training to or receiving from or participating in training with a listed terrorist organisation
- a person has been engaging in a hostile activity in a foreign country
- a person has been convicted of a terrorism offence in Australia
- a person has been convicted overseas for an offence that, if it occurred in Australia, would be a terrorism offence within the definition in subsection 3(1) of the Crimes Act
- the order would substantially assist in preventing the provision of support for or facilitation of a terrorist act, or
- the person has provided support for or otherwise facilitated the engagement in a hostile activity in a foreign country.

141. Each of the obligations, prohibitions and restrictions to be imposed on the person by the order must be reasonably necessary and reasonably appropriate and adapted for the purpose of:

- protecting 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 the facilitation of the engagement in a hostile activity in a foreign country.

142. The court therefore imposes only those requested conditions that would be necessary to fulfil one or more of the above purposes.

**Control orders and tracking devices**

143. Under subsection 104.5(1) of the *Criminal Code* a court may impose a requirement on a person to wear a tracking device as one of the obligations, prohibitions or restrictions of a control order. The court must be satisfied on the balance of probabilities that imposing such a requirement is reasonably necessary, and reasonably appropriate and adapted, for the purpose of protecting the public from a terrorist act, preventing the provision of support for, or the facilitation of a terrorist act or engagement in a hostile activity overseas.

144. The amendments to the control order regime in Division 104 of the *Criminal Code* ensure the effectiveness of this control in achieving these purposes by:

- requiring the subject of the control order to maintain the tracking device in good working order
- authorising the AFP to take steps, including entering specified premises, to ensure the tracking device and associated equipment are installed and maintained in good working order, and
- creating offences for interfering with the operation of a tracking device.

145. In order for the requirement to wear a tracking device to be effective, the tracking device must remain operational while the requirement is in place. The additional obligations, authorisations and prohibitions are designed to ensure the effectiveness of this control in protecting the public from, and mitigating the risk of occurrence of, a terrorist act.

*The right to freedom from arbitrary arrest or detention in Article 9 of the ICCPR*

146. Article 9 of the ICCPR provides that no-one shall be subjected to arbitrary arrest or detention or deprived of their liberty except on such grounds and in accordance with such procedure as are established by law. The UN Human Rights Committee has stated that 'arbitrariness' includes the elements of inappropriateness, injustice and a lack of predictability. An arrest or detention must be reasonable and necessary in all circumstances with reference to the recurrence of crime, interference with evidence or the prevention of flight.

147. The Bill engages the right to freedom from arbitrary detention as it creates new offences in section 104.27A of the *Criminal Code*, with maximum penalties of five years imprisonment. Penalties of up to five years imprisonment for interfering with the operation of a tracking device are the same as the penalty for contravening a term of a control order under existing section 104.27 of the *Criminal Code*. Parity of these penalties is appropriate given that all of the offences are directed to similar sorts of wrongdoing that frustrate and undermine the efficacy of the control order regime.

148. Any prosecution for an offence must be supported by admissible evidence and both the physical and fault elements proved to the criminal standard beyond reasonable doubt.

*The right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR*

149. Article 17 of the ICCPR provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.

150. Lawful interference with the right to privacy is permitted under Article 17 of the ICCPR, provided it is not arbitrary. In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be for a reason consistent with the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted the requirement of 'reasonableness' to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances.

151. The amendments allow an issuing court to authorise the AFP to enter premises for the purposes of installing equipment for the operation of the tracking device, and take steps specified in the order to ensure that the tracking device and associated equipment remain in

good working order. Entry to premises will engage, and limit, the protection from arbitrary and unlawful interference with privacy in Article 17.

152. The regime requires judicial authorisation of such action, and only after the issuing court has determined on the balance of probabilities that such a requirement is reasonably necessary, and reasonably appropriated and adapted for one of the purposes of protecting the public from, or mitigating the risk of, a terrorist act occurring.

153. The amendments provide that the issuing court may specify persons, times and places for the subject of the control order to report to for the purpose of having the tracking device inspected. Having this information specified as a term of the control order ensures that a person's compliance with certain terms of a control order cannot be examined at any time. It is intended to achieve a balance between the subject of the control orders' right to privacy and the need to ensure the effective operation of the tracking device.

154. Accordingly, the limitation on the right to privacy is reasonable, necessary and proportionate to the legitimate purpose of ensuring the efficacy of the requirement to wear a tracking device.

**Preventative detention orders**

155. The PDO regime is governed by Division 105 of the *Criminal Code*. Division 105 outlines the basis on which a PDO may be sought, the duration of the detention (no longer than 48 hours under the Commonwealth regime) and the rights and conditions associated with detention. The PDO regime seeks to achieve the legitimate objective of preventing an imminent terrorist act occurring and preserving evidence of, or relating to, a recent terrorist act. The imposition of a PDO is employed in emergency circumstances where traditional law enforcement powers are unavailable.

156. The amendments to the PDO regime contained in Schedule 5 are intended to clarify the required nature of the terrorist act under subsection 105.4(5) of the *Criminal Code*. The amendments achieve this by:

- replacing subsection 105.4(5) and the 'imminent test' with a threshold that focusses on the capability of a person to commit a terrorist act as opposed to the specific time the terrorist act is expected to occur, and
- clarifying that the thresholds applicable to the AFP member and issuing authority under subsection 105.4(4) apply to the requirements in subsection 105.4(5).

*Freedom from arbitrary detention and arrest in Article 9 of the ICCPR*

157. Article 9 of the ICCPR provides that no-one shall be subjected to arbitrary arrest or detention or deprived of their liberty except on such grounds and in accordance with such procedure as are established by law. The law itself should not be arbitrary and it must not be enforced in an arbitrary manner. In all instances, detention must be lawful, reasonable and necessary.

158. The amendments do not impact upon the right to freedom from arbitrary detention and arrest.

159. The right to freedom from arbitrary detention is safeguarded by the existing provisions in the PDO regime. These provisions continue to operate in conjunction with the amendments contained in Schedule 5. In particular, the basis for applying for a PDO and the proportionality requirements contained in subsection 105.4(4) mitigates the inappropriate imposition of a PDO. The application for a PDO requires that an AFP member must suspect, on reasonable grounds, that the person will engage in a terrorist act, possess a thing that is connected with the preparation for, or the engagement of a person in, a terrorist act or has done an act in preparation for, or is planning, a terrorist act (subparagraphs 105.4(4)(a)(i)-(iii)). The issuing authority must similarly be satisfied that there are 'reasonable grounds to suspect' the same matters (subparagraphs 105.4(4)(b)(i)-(iii)).

160. Having satisfied this threshold, the AFP member and issuing authority must also satisfy the proportionality tests contained in paragraphs 105.4(4)(c) and 105.4(4)(d). That is, they must demonstrate that a PDO will 'substantially assist' in preventing a terrorist act occurring (paragraph 105.4(4)(c)) and that detention for the period specified is 'reasonably necessary' for the purpose of preventing the terrorist act (paragraph 105.4(4)(d)). Law enforcement agencies must make out a case for why the limitations imposed by the PDO are justified in each circumstance. The cumulative effect of these provisions ensure that PDOs are only used in the most exceptional and extreme circumstances, where rapid preventative detention is reasonably necessary for preventing a terrorist act occurring, even where the timing of that terrorist act remains uncertain.

161. The amendments to the PDO regime do not adversely impact upon the freedom from arbitrary detention and arrest in Article 9 of the ICCPR.

***National Security Information (Criminal and Civil Proceedings) Act 2004***

**Protecting national security information in control order proceedings**

162. There are two parts to the amendments to the NSI Act contained in Schedule 15.

*Part 1 of Schedule 15 – Main amendments*

163. Part 1 provides for the enhanced protection of national security information in control order proceedings under Division 104 of the *Criminal Code*. Part 1 amends the NSI Act by enabling the court to make three new types of orders in control order proceedings for the making, confirming or varying of a control order. The effect of these orders is to allow information to be used in control order proceedings (subject to the rules of evidence) which is not disclosed to the subject of the control order and their legal representative.

164. The three new orders that may be made under revised section 38J in relation to a control order proceeding provide that:

- the subject of the control order and their legal representative may be provided a redacted or summarised form of the national security information. However, the court may consider all of the information contained in the original source document, even where that information has not been provided in the redacted or summarised form (new subsection 38J(2))

- the subject of the control order and their legal representative may not be provided with any information contained in the original source document. However, the court may consider all of that information (new subsection 38J(3)), or
- a witness may be called and the information provided by the witness need not be disclosed to the subject of the control order or their legal representative. However, the court may consider all of the information provided by the witness (new subsection 38J(4)).

165. The amendments also provide that at a closed hearing to determine whether one of the new orders should be made, the Attorney-General (or the Attorney-General's legal or any other representative) may request the court to order that one or more specified parties to the control order proceeding and their legal representatives not be present during the closed hearing. Even if the individual's legal representative is security cleared, the court may exclude them from the closed hearing, if the court considers it appropriate.

166. The amendments to the NSI Act pursue a legitimate objective, being the protection of national security information in control order proceedings where disclosure may be likely to prejudice national security. In light of the current threat environment, it is increasingly likely that law enforcement will need to rely on evidence that is extremely sensitive in nature, such that disclosure, even to a security-cleared lawyer, could compromise the safety of human sources and the integrity of ongoing police investigations. In the absence of the amendments contained in Part 1 of Schedule 15 there is a substantial risk that the inability to rely on, and protect, sensitive information may result in a control order being unable to be obtained against an individual who poses a risk to the safety of the community. This is because law enforcement would not be satisfied that existing protections under the NSI Act mitigate the risks associated with the disclosure of such information.

167. The speed of counter-terrorism investigations is increasing. In order for control orders to be effective, law enforcement agencies need to be able to act quickly, and to be able to present sensitive information (which is in the form of admissible evidence) to a court as part of a control order proceeding without risking the integrity, safety or security of the information or its source.

*Part 2 of Schedule 15 – Special advocates*

168. Part 2 of Schedule 15 creates a role for special advocates where the subject of a control order has sensitive information withheld from them (and their legal representative) as a result of an order under revised section 38J, and are excluded from parts of the control order proceeding when that information is considered by the court.

169. The appointment of a special advocate is at the discretion of the court, which is best placed to assess whether a special advocate is necessary to assist the court process and safeguard the rights of the subject of a control order. In some instances, the court may consider itself sufficiently equipped to safeguard the rights of the subject of a control order without the appointment of a special advocate. It is appropriate that that decision be made on a case by case basis when the Attorney-General seeks to protect information under revised section 38J.

170. The role of the special advocate is to represent the interests of the subject of a control order proceeding in parts of the control order proceeding from which they and their legal

representative have been excluded. The special advocate will be given the sensitive national security information the Attorney-General is either seeking to protect under an order under revised section 38J, or has obtained protection for as a result of a revised section 38J order. The special advocate has the powers necessary to represent the interests of the subject of a control order effectively in closed hearings. These powers are:

- making submissions to the court at any part of a hearing in the proceeding during which the party and the party's legal representative are not entitled to be present
- adducing evidence and cross-examining witnesses at such part of a proceeding, and
- making written submissions to the court.

171. Before receiving the sensitive information, the special advocate will generally be able to communicate without any restriction with the subject of a control order and their legal representative. Following the receipt of the sensitive information, the special advocate will only be able to communicate with the subject of the control order in writing and with the approval of the court. The special advocate will not be able to disclose to the subject of the control order or their legal representative the content of the sensitive information provided to them. The subject of a control order and their legal representative will be able to continue to communicate with the special advocate. However, communications must be in writing and in the case of the subject of a control order, only through their legal representative.

*The right to a fair hearing in Article 14(1) of the ICCPR*

172. The amendments to the NSI Act apply only in relation to proceedings under Division 104 of the *Criminal Code* for the making, confirming and varying of a control order. These proceedings are suits at law for the purposes of Article 14 of the ICCPR. The withholding of information from a subject of a control order impacts upon Article 14(1) of the ICCPR, which safeguards the right to a fair hearing in a suit at law. In particular, the amendments to the NSI Act may limit the equality of arms principle which requires that all parties to a proceeding must have reasonable opportunity of presenting their case under conditions that do not disadvantage them against other parties to the proceeding.

173. However, it is important when considering the impact on an individual's right to a fair trial that the proposed amendments be considered as a whole rather than in isolation. While the new orders provided under revised section 38J depart from ordinary instances of procedure and judicial process, the incorporation of a role for special advocates and the inherent capacity of the court to act fairly and impartially as well as the safeguards built into the NSI Act provide several mechanisms through which a fair hearing is guaranteed. These mechanisms are outlined below.

174. Firstly, the involvement of the special advocate provides a significant safeguard against the contravention of the equality of arms principle. The special advocate will be able to see the sensitive information that has been withheld from the subject of a control order. While the special advocate cannot communicate to the subject of a control order about that information or take instructions in relation to that information, the special advocate will still be able to make arguments querying the need to withhold that information from the subject of a control order (and their legal representative) and can challenge the relevance, reliability and weight accorded to that information.

175. The restrictions on the ability of the special advocate to communicate the sensitive information to the subject of a control order is a reasonable, necessary and proportionate measure in order to protect highly sensitive information. The unauthorised disclosure of that information may disrupt ongoing law enforcement or intelligence operations, reveal technologies and methods used to collect and analyse intelligence, endanger the lives of human sources or adversely impact upon Australia's relationships with its international partners. Despite these communication restrictions, the involvement of a special advocate protects the subject of a control order's right to a fair trial and enhances the degree of procedural fairness they are afforded.

176. Secondly, in determining whether to make an order under revised section 38J, the court must be satisfied that the subject (or proposed subject) of the control order has been given 'sufficient information about the allegations on which the control order request was based to enable effective instructions to be given in relation to those allegations'. What constitutes 'sufficient' information will be determined on a case-by-case basis.

177. This minimum standard of disclosure of information ensures that the subject of the control order has sufficient knowledge of the essential allegations on which the control order request is sought (or varied), such that they are able to dispute those allegations during the substantive control order proceedings. Where this level of information is provided, the subject's right to a fair trial will be satisfied, notwithstanding that they may not be provided with the detail or sources of the evidence forming the basis of the allegations against them.

178. Thirdly, in determining whether to make an order under new section 38J, the court must have regard to the following factors:

- the potential prejudice to national security in not making one of the orders under new section 38J (paragraph 38J(5)(a))
- whether the making of an order under new section 38J would have a 'substantial adverse effect on the substantive hearing in the proceeding' (paragraph 38J(5)(b)), and
- any other matter the court considers relevant (paragraph 38J(5)(c)).

179. The requirement to give consideration to the adverse effect on the substantive hearing ensures that the court expressly contemplates the effect of any potential order under revised section 38J on a party's ability to receive a fair hearing. The case-by-case basis on which such an assessment is made provides the court with the discretion to adequately assess the impact of an order under revised section 38J on each subject (or proposed subject) of the control order.

180. Fourthly, the NSI Act guarantees procedural fairness by preserving the discretion of the court. The amendments to the NSI Act do not compel the court to make any of the orders that may be sought under Schedule 15. The court may decline making an order under revised section 38J, or where it does make an order, the court may determine what form such an order may take (for instance, whether there should be redactions or summaries of information provided). Similarly, the court has the discretion under new subsection 38I(3A) to decline excluding specified parties and their legal representatives from the closed hearing proceedings.

181. The amendments in Schedule 15 also preserve the right of the court to stay a control order proceeding where one of the new orders under revised section 38J has been made and the order would have a substantial adverse effect on the substantive control order proceeding. Accordingly, even where the court has made an order under revised section 38J, the court is not prevented from later determining that the operation of the order is such that it compromises the ability of the subject (or proposed subject) of the control order the right to receive a fair hearing.

182. Furthermore, existing subsection 19(3) preserves the power of the court to control the conduct of civil proceedings, in particular with respect to abuse of process unless the NSI Act expressly or impliedly provides otherwise. Where a legislative scheme departs from the general principles of procedural fairness, the question for the judiciary will be whether, taken as a whole, the court's procedures for resolving the dispute accord both parties procedural fairness and avoid practical injustice. The discretion provided to the court in managing a control order proceeding enables the court to assess at each stage of the proceeding, whether the subject of a control order has been afforded procedural fairness.

183. Finally, the normal rules of evidence will continue to apply to evidence sought to be introduced under the new orders contained in revised section 38J, in accordance with that section and existing *Criminal Code* provisions (section 104.28A). Where evidence is withheld from the subject of a control order, that evidence must be admissible pursuant to the rules of evidence applicable in control order proceedings. Moreover, the amendments in Schedule 15 do not dictate to the court what weight it should give to any evidence that is withheld (either in full or in part) from the subject of the control order in the substantive control order proceeding.

184. The amendments to the NSI Act achieve the legitimate objective of protecting national security information in control order proceedings, the disclosure of which may be likely to prejudice national security. The protection of national security information can be vital, not only in maintaining the confidentiality and integrity of law enforcement and intelligence operations and methodologies, but also in maintaining the trust with which such information has been provided to law enforcement. However, the imperatives of protecting national security information under Schedule 15 do not deprive the subject of a control order proceeding of procedural fairness. The fundamental right to a fair hearing in a suit at law guaranteed by Article 14(1) of the ICCPR is upheld as a result of: the role of the special advocate when the amendments contained in Part 1 of Schedule 15 are enlivened, the safeguards contained in Schedule 15 and the existing provisions of the NSI Act, which provide the court options for redressing any unfairness that may arise during a control order proceeding where national security information is sought to be protected.

***Surveillance Devices Act 2004***

185. The SD Act regulates the use of surveillance devices. It establishes procedures for law enforcement officers to obtain surveillance device warrants for the purposes set out in section 14 (offence investigations, child recovery orders, mutual assistance investigations and integrity operations). Surveillance device warrants have not however been available to law enforcement agencies for monitoring control orders. This is problematic because some control order conditions cannot effectively be monitored without electronic surveillance.

186. The proposed new monitoring warrants within the SD Act will apply to individuals subject to a control order under Division 104 of the *Criminal Code*. Unlike the existing

surveillance device warrant regime, the new regime will not require the issuing authority to be satisfied that one or more relevant offences have been, are being, are about to be, or are likely to be, committed. Rather, this regime will allow law enforcement officers to apply to an issuing authority for a surveillance device warrant for the purposes of monitoring compliance with a control order issued under Division 104. It will allow surveillance device information to be used in any proceedings associated with that control order.

187. The new regime will also extend the circumstances in which agencies may use less intrusive surveillance devices without a warrant to include monitoring of a control order. It will also allow protected information obtained under a control order warrant to be used to determine whether the control order has been complied with.

188. The power to use surveillance devices for monitoring purposes will remain a covert power. The amendments will introduce new deferred reporting arrangements, which will permit the chief officer of an agency to defer public reporting on the use of a monitoring warrant in certain circumstances, balancing the public interest in timely and transparent reporting with the public interest in preserving the effectiveness of this covert power.

189. The Bill allows a law enforcement officer to apply for, or authorise, a surveillance device warrant if the officer suspects on reasonable grounds that the use of a surveillance device would be likely to substantially assist in the purpose of:

- protecting the public from a terrorist act
- preventing the provision of support for, or the facilitation of, a terrorist act
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

190. The Bill permits the limited use of protected information obtained under a control order warrant relating to an interim control order which is subsequently declared void. The information may be used, communicated, recorded or given in evidence in a proceeding when it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, serious damage to property or a purpose connected with a Commonwealth, state or territory PDO regime.

191. This limited permission to use information obtained on the basis of an interim control order that has been declared void reflects the significant public interest in protecting members of the public from terrorist acts or serious harm, and in preventing serious damage to property. Notwithstanding that the underlying order in relation to which the warrant was made is no longer valid, there remains a strong justification for allowing the information be used to prevent significant harm to the public. To provide otherwise would frustrate the protection of the community where information obtained in good faith must be relied on to prevent or reduce the commission of a terrorist act or other related serious harm.

*The right to life and security of the person in Articles 6 and 9 of the ICCPR*

192. The Bill promotes the right to life and the right to security of the person. The right to security of the person in Article 9 of the ICCPR requires states to provide reasonable and appropriate measures to protect a person's physical security. The right to life also places a

positive obligation on states to protect individuals from unwarranted actions by private persons, such as acts of terrorism. The obligation to protect life requires the State to take preventative operational measures to protect individuals whose safety may be compromised in particular circumstances, such as by a terrorist act. This includes enhancing the capabilities of law enforcement agencies to respond to a heightened terrorist threat.

193. The risk of persons subject to control orders continuing to engage in preparatory acts has intensified due to changes in the threat environment. Terrorism is increasingly conducted by smaller groups or lone actors engaging in short-term, low-complexity attack plans, reducing the warning time for attacks, and the ability for agencies to detect, investigate and disrupt attacks before they occur. From a counter-terrorism perspective, the number of persons of concern in Australia is substantially higher than at any point historically, and is expected to increase substantially if, and when, foreign fighters return, placing exceptionally high pressure on agencies. Similarly, returning foreign fighters will necessarily impact the domestic threat environment given their combat and tradecraft experience, and established terrorist networks.

194. Articles 6 and 9 require states to take positive steps to protect individuals' physical security. This can include enhancing the capabilities of law enforcement agencies to respond to a heightened terrorist threat. The amendments to the SD Act enable law enforcement agencies to better detect, monitor and investigate potential terrorist threats in this heightened threat environment. By enhancing the access to surveillance devices to monitor compliance with control orders, agencies can identify risks early and intervene to prevent an act of terrorism.

*The right to a fair trial and fair hearing under Article 14 of the ICCPR*

195. Article 14 of the ICCPR protects an individual's right to a fair trial and fair hearing. The right applies to both criminal and civil proceedings and to cases before both courts and tribunals. The right is concerned with procedural fairness and encompasses notions of equality in proceedings, the right to a public hearing and the requirement that hearings are conducted by an independent and impartial body.

196. The Bill engages this right by inserting a provision which enables agencies to use protected information obtained under a surveillance device warrant relating to an interim control order which is subsequently declared void. The information may be used, communicated, recorded or given in evidence in a proceeding when it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, serious damage to property or a purpose connected with a Commonwealth, state or territory PDO regime (for example, for the purposes of preparing and applying for a PDO to prevent an imminent terrorist act).

197. The provision is intended to address the unlikely scenario where:

- an interim control order has been issued in respect of a person
- a law enforcement agency has duly obtained a control order warrant in relation to that person
- under that control order warrant, the agency has obtained information that indicates that the person is likely to engage in a terrorist act, cause serious harm to a person, or cause serious damage to property, and

- before the agency can act on that information, the interim control order is considered by a court at a confirmation hearing and declared void *ab initio* pursuant to subsection 104.14(6) of the *Criminal Code* on the grounds that, at the time of making the interim control order, there were no grounds on which to make the order.

198. As the existence of a valid control order is a condition for the issuing of a control order warrant, the likely effect of a court declaring an interim control order void *ab initio* pursuant to subsection 104.14(6) of the *Criminal Code* would be that any control order warrants predicated on that control order would also likely be void *ab initio*.

199. It is a fundamental principle of the Australian legal system that courts have a discretion as to whether or not to admit information as evidence into proceedings, irrespective of the manner in which the information was obtained. As an example, the *Bunning v Cross*[1] discretion places the onus on the accused to prove misconduct in obtaining certain evidence and to justify the exclusion of the evidence. This principle is expanded on in Commonwealth statute,[2] where there is an onus on the party seeking admission of certain evidence to satisfy the court that the desirability of admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. This fundamental principle reflects the need to balance the public interest in the full availability of relevant information in the administration of justice against competing public interests, and demonstrates the role the court plays in determining admissibility of evidence.

200. However, the SD Act departs from these fundamental principles, by imposing strict prohibitions on when material under those Acts may be used, communicated or admitted into evidence.[3] Under the SD Act, it is a criminal offence for a person to deal in information obtained under these Acts for any purpose, unless the dealing is expressly permitted under one or more of the enumerated and exhaustive exceptions to the general prohibition. This prohibition expressly overrides the discretion of the judiciary, both at common law and under the Evidence Act, to admit information into evidence where the public interest in admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. There is also a risk that the prohibition might be interpreted, either by a court considering the matter after the fact, or by an agency considering the question *in extremis*, to override the general defence to criminal responsibility under the *Criminal Code*.

201. For this reason, the amendment does not infringe on the right to a fair trial and fair hearing as protected by article 14 of the ICCPR. 'Equality of arms' requires that each party be afforded a reasonable opportunity to present their case under the conditions that do not place them at a substantial disadvantage vis-à-vis another party.[4] This principle essentially denotes equal procedural ability to state the case. This amendment does not engage the 'equality of arms' principle. This is because the amendment does not derogate from, or abridge, existing procedural rights of parties to litigation and would not result in actual disadvantage or other unfairness to the defendant. That is, the amendment does not impact

---

[1] (1978) 141 CLR 54.
[2] Section 138 of the *Evidence Act 1995* (Cth).
[3] See s 45 of the SD Act.
[4] *Brandstetter v Austria*, Application No: 11170/84; 12876/87; 13468/87, Strasbourg judgment 28 August 1991 §§41-69.

upon opportunities to adduce or challenge evidence or present arguments on the matters at issue.[5]

202. Accordingly, the provisions are a reasonable and proportionate limitation on the right to a fair trial and fair hearing in article 14 of the ICCPR.

*The right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR*

203. Article 17 of the ICCPR prohibits arbitrary or unlawful interference with an individual's privacy, family, home or correspondence. This right may be subject to permissible limitations where those limitations are provided by law and non-arbitrary. In order for limitations not to be arbitrary, they must be aimed at a legitimate objective and be reasonable, necessary and proportionate to that objective.

204. To justify a limitation of human rights, a legitimate objective must address a pressing or substantial concern and not simply seek an outcome that is desirable or convenient. The Bill is intended to enhance law enforcement agencies' abilities to prevent, detect and investigate acts of terrorism. Terrorism is a significant threat to national security and public safety for a variety of reasons. Firstly, politically motivated, violent acts can indiscriminately threaten the lives and physical safety of Australian citizens. This can perpetuate a climate of fear which is socially divisive, threatening the cohesiveness of Australian society. Not only does terrorism undermine national security and community safety, it also damages the cohesiveness of Australian society more generally.

205. The current threat environment has meant that terrorism has become a substantial concern for law enforcement agencies and Australian society more generally. The nature of terrorism itself is changing with smaller groups or lone actors engaging in short-term, low-complexity attack plans, reducing the warning time for attacks. From a counter-terrorism perspective, the number of persons of concern in Australia is substantially higher than at any point historically, and is expected to increase substantially if, and when, foreign fighters from the Syrian conflict return. In light of this, the prevention of terrorism is a legitimate objective.

206. The limited extension of the use of surveillance devices ensures that these amendments are reasonable and proportionate. Surveillance devices powers are intrusive and covert in nature, and can potentially intrude on the privacy of persons other than the person subject to the control order.

207. The purpose of the control order regime is to address the challenge posed by terrorism and hostile activity in foreign countries by mitigating the threat posed by specific, high-risk individuals.

208. The use of surveillance devices to monitor those subject to control orders will better ensure compliance with conditions imposed, and better mitigate the risk of terrorism and involvement in foreign conflicts. If a person subject to a control order perceives there is little

[5] *H. v Belgium*, Application No: 8950/80, Strasbourg judgment 30 November 1987 §§49-55.

likelihood of breaches being detected, there is little incentive for them to moderate their behaviour, and the specific deterrence effect of a control order is potentially undermined.

209. Under the current law, agencies have limited means to monitor a person's compliance with a control order, and to detect planning and preparatory acts for a terrorist act or hostile activity overseas. At present, agencies are often limited to physical surveillance, which is ineffective in many cases and is exceptionally difficult to scale due to its resource-intensive nature.

210. The new provisions will allow law enforcement officers to apply to an issuing authority for a surveillance device warrant for the purposes of monitoring a person subject to a control order, to prevent or protect the public from terrorism or prevent a person from assisting hostile activity in a foreign country.

211. The amendments establish a number of safeguards to ensure that any interference with privacy is for a legitimate objective and implemented in a proportionate manner. Agencies are required to apply to an eligible judge or nominated AAT member for a warrant authorising the use or installation of a surveillance device, where entry into a premises or interference with a vehicle without the owner's permission is required. Independent oversight prior to the use of a privacy-intrusive surveillance device requires law enforcement agencies to demonstrate the necessity and proportionality of surveillance to an independent party. This is an important safeguard.

212. Agencies are not automatically entitled to receive control order warrants in relation to persons who are subject to control orders. Before issuing a control order warrant, the independent issuing authority must be satisfied inter alia that the use of a surveillance device would be likely to substantially assist in one or more of the purposes for which a control order warrant may be issued, being:

- protecting the public from a terrorist act; or
- preventing the provision of support for, or the facilitation of, a terrorist act; or
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

213. Even where the issuing authority is satisfied that the use of a surveillance device would be likely to substantially assist in one or more of the above purpose, the issuing authority is not required to issue a control order warrant. The decision to issue a control order monitoring warrant is discretionary, and may only be taken after the issuing authority has had regard to a range of competing public interests, including:

- the extent to which the privacy of any person (including third parties) is likely to be affected;
- the existence of alternative means of obtaining the evidence or information sought to be obtained;
- whether the use of a surveillance device is likely to have the least interference with the privacy of any person of any means of obtaining the evidence or information;

- the likely value of the information sought to be obtained in relation to the relevant purpose(s) for issuing the warrant;
- the likelihood that the person subject to the control order has engaged in, is engaging in, or will engage in, the conduct that sought to be detected and prevented by the control order warrant; and
- any previous control order warrants issued in relation to the person.

214. The requirement to 'have regard to' the above matters requires the issuing authority to give those matters a proper, genuine and realistic consideration, and amounts to a requirement for the issuing authority to consider both the necessity for the control order warrant (including the likelihood that the person has engaged in, is engaging in, or will engage in conduct that is sought to be detected and prevented by the warrant, and the likely value of the information that is sought to be obtained, in light of any previous control order warrants issued in relation to the person) and the proportionality of issuing the control order warrant (including the likely degree of interference with the privacy of the person subject to the control order and any third parties, and the availability of alternative, less intrusive methods).

215. In some circumstances, law enforcement officers may authorise the use of a surveillance device without a warrant. The SD Act allows the use of optical surveillance, listening and tracking devices without a warrant in circumstances which do not involve covert entry onto premises or interference with a vehicle. For instance, an officer may use an optical surveillance device in a public place without a warrant. There is a lower threshold for the use of these devices because they are less privacy-intrusive than circumstances where the use of the device requires entry into an individual's premises or vehicle without permission. The Bill does not alter the categories of surveillance devices for which warrants are required, rather it allows all surveillance devices to be used, whether authorised by warrant or not, to monitor compliance with a control order.

216. Strict limitations upon when surveillance devices can be used to enforce control orders ensures that they are only used where they are necessary. The amendments compel the immediate revocation of a warrant and discontinuance of surveillance if it is no longer necessary for the purposes of the investigation, or where the control order is no longer in force.

217. A law enforcement officer can apply for a surveillance device warrant after the control order has been made but before it has come into force by being served on the subject of the order. Likewise, the surveillance device warrant can be issued during this period. This is intended to ensure that officers have an opportunity to install surveillance devices covertly, as there are often limited opportunities to do so. This provision also ensures that monitoring powers are in place before the control order comes into force to avoid the loss of evidence due to a delay in service of the control order warrant. The purposes for which information obtained by way of a surveillance device during this intervening period may be used are strictly limited: agencies are required to destroy information obtained during this period, unless the chief officer of the agency is satisfied that it is likely to assist with the protection of the public from a terrorist act, prevent the provision of support for, or the facilitation of, a terrorist act, or the provision of support for, or the facilitation of, the engagement in hostile activities in a foreign country. The ability to use information obtained prior to the entry-into-force of a control order in these circumstances is a legitimate and proportionate use of surveillance in light of the gravity of the terrorist threat.

218. The amendments contain important record-keeping measures which enhance oversight of the regime. The chief officer of each law enforcement agency is required to report to the Minister on the benefits of surveillance device warrants issued to monitor compliance with a control order. This reporting measure is designed to encourage transparency, by revealing the purposes for which surveillance devices are used and detailing their contribution to the prevention of terrorist acts.

219. The amendments will also introduce new deferred reporting arrangements which will permit the chief officer of an agency to delay public reporting on the use of a surveillance device warrant in relation to a control order in certain circumstances. Due to the small number of control orders which are issued, immediate reporting of any warrants or authorisations of surveillance devices may enable an individual to determine whether they are the subject of surveillance. If a person knows, or suspects that there is a control order surveillance device warrant in place, they are more likely to be able to modify their behaviour to defeat those lawful surveillance efforts. Also, if a person knows or suspects that a surveillance device warrant is not in force, the deterrence value of the control order is limited to the extent that the person believes they can engage in proscribed activity without risk of detection. Deferred reporting balances the public interest in timely and transparent reporting with the need to preserve the effectiveness of control orders to prevent individuals from committing terrorist acts.

220. The Bill will place strict controls on the decision to defer public reporting on the use of control order warrants, reflecting the significant public interest in transparency in relation to the use of exceptional, covert powers. First, the decision to defer public reporting may only be made by the Minister, on the advice of the chief officer of the relevant agency. Second, the chief officer and the Minister must each be satisfied that publicly reporting particular information could be reasonably expected to enable a reasonable person to determine that particular surveillance measures are likely to be, or not to be in force at the time he or she makes his or her decision (which will generally be at different times, given the time taken to prepare the Minister's report based on all agencies' input). Third, where public reporting is deferred in relation to particular information, the chief officer of the relevant agency will be required to reconsider his or her decision each year. Fourth, documentary records must be kept in relation to each such decision. Fifth, each such decision is subject to independent oversight by the Commonwealth Ombudsman.

221. The Bill also allows for the use, recording, communication or publication, or admission into evidence of protected information for the purposes of proceedings arising under, or in relation to control orders and PDOs. These amendments are intended to clarify that protected information can be used in such proceedings, including applications for, appeals against, and civil proceedings in relation to control orders and PDOs. This recognises the importance of protected information to applications for such orders and ensures that covertly collected information can be used in control order and related proceedings.

222. The information obtained from a surveillance device may only be used for the clearly defined purpose of obtaining either a control order or a PDO. Such orders are utilised by national security and law enforcement agencies to prevent the public from a terrorist act. In light of the changing nature and increased risk of terrorism, as detailed above, interference with the privacy of persons who are the subject of a control order is legitimate and proportionate to the objective of protecting the broader community from terrorism.

*The right to freedom of expression in Article 19 of the ICCPR*

223. Article 19 of the ICCPR provides that all persons shall have the right to freedom of expression, including the freedom to speak, receive and impart information and ideas of all kinds, through any media of a person's choice. This right may be subject to restrictions for the purposes of national security or public order where such restrictions are provided by law and are clearly necessary.

224. This Bill engages the right to freedom of expression indirectly, to the extent that individuals subject to control orders may suspect that their communications are being monitored. This suspicion may cause them to restrict their communications, both in terms of content and audience. The nature of the terrorism threat is evolving, with rapid radicalisation and low sophistication attacks resulting in shorter timeframes for agencies to detect and disrupt attacks. Furthermore, returning foreign fighters will necessarily impact the domestic threat environment given their combat and tradecraft experience, and established terrorist networks. This heightened risk justifies any indirect limitation on free speech for a limited number of specific individuals subject to control orders.

*The right to an effective remedy in Article 2(3) of the ICCPR*

225. Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights or freedoms recognised by the ICCPR, including the right to have such a remedy determined by the competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the State. The right to an effective remedy applies notwithstanding that a violation has been committed by persons acting in an official capacity.

226. The right to an effective remedy applies in relation to violations of other ICCPR rights and freedoms. By establishing a new control order monitoring warrant regime, the Bill indirectly creates a risk that a person's right to protection against arbitrary and unlawful interferences with privacy under Article 17 of the ICCPR may be violated where a surveillance device is used in connection with a control order, or information obtained under monitoring warrant or authorisation is used, in a manner that is unlawful. Accordingly, the Bill engages the right to an effective remedy for any such violation of the right to privacy.

227. The Bill engages the right to an effective remedy by providing immunity, including immunity for ancillary conduct, in limited circumstances, for conduct that could otherwise found a criminal charge. The Bill protects persons from criminal liability for acts done, or omitted to be done, in good faith purportedly under the authority of the SD Act in connection with an interim control order that has subsequently been declared to be void.

228. The scheme is necessary to ensure the effective performance of the statutory functions of law enforcement agencies, by ensuring that law enforcement officers can be confident that they will not face criminal liability for conduct engaged in in good faith:

- under a legal authority provided by the SD Act that is valid at the time the officer engages in the conduct, or
- under a legal authority provided by the SD Act that the officer reasonably believes to be valid at the time the officer engages in the conduct.

229. Not providing this immunity would impair law enforcement agencies' capabilities and willingness to ensure a safe and secure Australia. Because a Court may declare an interim control order void *ab initio*, absent an immunity, law enforcement officers would potentially face retrospective criminal liability for conduct they engaged in, in good faith, in reliance on a legal authority that was valid at the time. The existence of such a risk would create a powerful deterrent for officers to rely on valid legal authorities.

230. The limitation to the right to an effective remedy is limited to the extent that it is reasonable, necessary and proportionate to the objective of facilitating the fulfilment of law enforcement agencies' functions in protecting the public from acts of terrorism, preventing the engagement in hostile activities in foreign countries, and monitoring persons' compliance with control orders. The immunity is limited to conduct engaged in, in good faith, and does not apply if, at that time, the person knew, or ought reasonably to have known, that the interim control order underpinning the legal authority provided by the SD Act had been declared void. In particular, the Bill also does not immunise law enforcement agencies (which would ordinarily assume vicarious liability for acts done or omitted to be done by their officers) from civil liability for any such conduct; persons may therefore seek civil remedies for damage or harm suffered as a result of any act done, or omitted to be done, under the authority of the SD Act where that authority was dependent upon the existence of an interim control order that has subsequently been declared void.

231. The SD Act protects this right by ensuring the Commonwealth Ombudsman has robust oversight powers enabling it to compel authorised agencies and individuals to answer questions and provide information. A person may face imprisonment of up to two years if they use, record, communicate or publish protected information outside the purposes permitted in the SD Act.

***Taxation Administration Act 1953***

**Authorised disclosure to an Australian government agency for purposes related to national security**

232. Subsection 355-65(2) of Schedule 1 of the TA Act provides for the disclosure of protected information for certain purposes relating to social welfare, health or safety. The amendment supplements existing exemptions, authorising taxation officers to record or disclose protected information to an Australian government agency for the purposes of preventing, detecting, disrupting or investigating conduct that relates to a matter of security as defined by section 4 of the ASIO Act.

233. Consistent with Item 9 of Table 1 at subsection 355-65 of Schedule 1 to the TA Act, this amendment will allow taxation officers to disclose information to an Australian government agency, for certain specified purposes. It is important that the amendment allows the ability to disclose information, for the purposes of preventing, detecting, disrupting or investigating conduct that relates to a matter of security, to 'any' Australian government agency because bodies that have a role in dealing with national security threats vary from time to time. In addition, bodies such as the National Disruption Group are multi-jurisdictional and their composition can change at short notice.

234. This amendment recognises that the public interest in allowing government agencies to use information, to prevent, detect, disrupt or investigate conduct that relates to a matter of security, outweighs the associated loss of privacy.

235. Following Recommendation 20 of the Committee advisory report, new section 355-182 provides an important safeguard in the form of the ability of an Australian government agency officer to disclose protected taxation information to the Commonwealth Ombudsman where the Ombudsman has not sought that information under section 9 of the *Ombudsman Act 1976* (the Ombudsman Act).

*The right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR*

236. For the purposes of the exceptions under the new section 355-182, the recording or disclosure of information must be necessary or appropriate for purposes of preventing, detecting, disrupting or investigating conduct related to security, as defined by section 4 of the ASIO Act. Similar provisions already exist for serious threats to an individual's life, health or safety or public health or public safety and this is an extension of that power. The disclosure is for a limited purpose and is neither arbitrary nor unlawful. Taxation officers may only disclose protected information after the provision commences, but the provision authorises disclosure of information collected before commencement of the Bill.

237. The exceptions to the disclosure prohibitions are designed having regard to the principle that disclosure of taxpayer information should be permitted only where the public benefit associated with the disclosure clearly outweighs the need for taxpayer privacy.

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

238. The TIA Act allows the AFP to use, communicate or give lawfully intercepted information in evidence in relation to the Commonwealth PDO regime. The Bill will enable state and territory agencies to use or communicate lawfully intercepted information in relation to their respective PDO regimes. This will ensure consistency between the Commonwealth's PDO regime and the states and territories' regimes in the following Acts:

- *Terrorism (Community Protection) Act 2003* (Vic)
- *Terrorism (Police Powers) Act 2002* (NSW)
- *Terrorism (Preventative Detention) Act 2005* (Qld)
- *Terrorism (Preventative Detention) Act 2005* (SA)
- *Terrorism (Preventative Detention) Act 2005* (Tas)
- *Terrorism (Preventative Detention) Act 2006* (WA)
- *Terrorism (Extraordinary Temporary Powers) Act 2006* (ACT), and
- *Terrorism (Emergency Powers) Act 2003* (NT).

239. The Bill ensures that an officer or staff member of a state or territory agency who previously communicated, made use of, or made a record of lawfully intercepted information for a purpose that would now be covered by the amendment above would be taken not to have contravened the prohibition on communicating lawfully intercepted information. This will ensure that any officer who has in good faith used or communicated lawfully intercepted information for a purpose connected with state and territory PDO legislation is not liable for a breach of the TIA Act.

240. The Bill permits the limited use of either lawfully intercepted information or lawfully accessed information obtained under a control order warrant relating to an interim control order which is subsequently declared void. The information may be used, communicated, recorded or given in evidence in a proceeding when it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, serious damage to property or a purpose connected with a Commonwealth, state or territory PDO regime.

241. This limited permission to use information obtained on the basis of an interim control order that has been declared void reflects the significant public interest in protecting members of the public from terrorist acts or serious harm, and in preventing serious damage to property. Notwithstanding that the underlying order in relation to which the warrant was made is no longer valid, there remains a strong justification for allowing the information be used to prevent significant harm to the public. To provide otherwise would frustrate the protection of the community where communications intercepted in good faith must be relied on to prevent or reduce the commission of a terrorist act or other related serious harm.

*The right to life in Article 6 of the ICCPR and the right to liberty and security of the person in Article 9 of the ICCPR*

242. The Bill promotes the right to life in Article 6 of the ICCPR and the right to security of the person in Article 9. The right to security of the person requires states to provide reasonable and appropriate measures to protect a person's physical security. The right to life also places a positive obligation on states to protect individuals from unwarranted actions by private persons, such as acts of terrorism. The obligation to protect life requires the State to take preventative operational measures to protect individuals whose safety may be compromised in particular circumstances, such as by a terrorist act. This includes enhancing the capabilities of law enforcement agencies to respond to a heightened terrorist threat.

243. In the existing threat environment, there is a risk that persons subject to control orders may continue to engage in preparatory acts of terrorism. Terrorism is increasingly conducted by smaller groups or lone actors engaging in short-term, low-complexity attack plans, reducing the warning time for attacks, and the ability for agencies to detect, investigate and disrupt attacks before they occur. From a counter-terrorism perspective, the number of persons of concern in Australia is substantially higher than at any point historically, and is expected to increase substantially if, and when, foreign fighters return, placing exceptionally high pressure on agencies. Similarly, returning foreign fighters will necessarily impact the domestic threat environment given their combat and tradecraft experience, and established terrorist networks.

244. Articles 6 and 9 require states to take positive steps to protect individuals' physical security. This can include enhancing the capabilities of law enforcement agencies to respond to a heightened terrorist threat. The amendments to the TIA Act enable law enforcement agencies to better detect, monitor and investigate potential terrorist threats in the heightened threat environment. By enhancing the access to interception to monitor compliance with control orders, agencies can identify risks early and intervene to prevent an act of terrorism.

245. As noted above, returning foreign fighters will necessarily impact the domestic threat environment given their combat and tradecraft experience, and established terrorist networks. Narrowly expanding the grounds on which law enforcement agencies can undertake interception of those subject to control orders will enable them to monitor 'at risk' individuals

who have extensive links to terrorist groups, identify potential risks and intervene to prevent an act of terrorism.

246. The amendments allow lawfully intercepted information to be dealt with in relation to state and territory PDOs, and allow lawfully intercepted information obtained under a warrant relating to a control order that is declared void to be used, communicated, recorded or given in evidence in a proceeding when it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, serious damage to property or a purpose connected with a Commonwealth, state or territory PDO regime. This will assist national security and law enforcement agencies to identify terrorism risks early, investigate potential terrorist threats, and thereby prevent an act of terrorism from occurring. Similarly, it will enable agencies to act to prevent individuals from involvement in hostile activity overseas.

*The right to a fair trial and fair hearing under Article 14 of the ICCPR*

247. Article 14 of the ICCPR protects an individual's right to a fair trial and fair hearing. The right applies to both criminal and civil proceedings and to cases before both courts and tribunals. The right is concerned with procedural fairness and encompasses notions of equality in proceedings, the right to a public hearing and the requirement that hearings are conducted by an independent and impartial body.

248. The Bill engages this right by inserting a provision which enables agencies to further use either lawfully intercepted information or lawfully accessed information obtained under an interception warrant relating to an interim control order which is subsequently declared void. The information may be used, communicated, recorded or given in evidence in a proceeding when it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, serious damage to property or a purpose connected with a Commonwealth, state or territory PDO regime (for example, for the purposes of preparing and applying for a PDO to prevent an imminent terrorist act).

249. The provision is intended to address the unlikely scenario where:

- an interim control order has been issued in respect of a person
- a law enforcement agency has duly obtained a control order warrant in relation to that person
- under that control order warrant, the agency has obtained information that indicates that the person is likely to engage in a terrorist act, cause serious harm to a person, or cause serious damage to property, and
- before the agency can act on that information, the interim control order is considered by a court at a confirmation hearing and declared void *ab initio* pursuant to subsection 104.14(6) of the *Criminal Code* on the grounds that, at the time of making the interim control order, there were no grounds on which to make the order.

250. As the existence of a valid control order is a condition for the issuing of a control order warrant, the likely effect of a court declaring an interim control order void *ab initio* pursuant to subsection 104.14(6) of the *Criminal Code* would be that any control order warrants predicated on that control order would also likely be void *ab initio*.

251. It is a fundamental principle of the Australian legal system that courts have a discretion as to whether or not to admit information as evidence into proceedings, irrespective of the manner in which the information was obtained. As an example, the *Bunning v Cross*[6] discretion places the onus on the accused to prove misconduct in obtaining certain evidence and to justify the exclusion of the evidence. This principle is expanded on in Commonwealth statute,[7] where there is an onus on the party seeking admission of certain evidence to satisfy the court that the desirability of admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. This fundamental principle reflects the need to balance the public interest in the full availability of relevant information in the administration of justice against competing public interests, and demonstrates the role the court plays in determining admissibility of evidence.

252. However, the TIA Act departs from these fundamental principles, by imposing strict prohibitions on when material under those Acts may be used, communicated or admitted into evidence.[8] Under the TIA Act, it is a criminal offence for a person to deal in information obtained under these Acts for any purpose, unless the dealing is expressly permitted under one or more of the enumerated and exhaustive exceptions to the general prohibition. This prohibition expressly overrides the discretion of the judiciary, both at common law and under the Evidence Act, to admit information into evidence where the public interest in admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. There is also a risk that the prohibition might be interpreted, either by a court considering the matter after the fact, or by an agency considering the question *in extremis*, to override the general defence to criminal responsibility under the *Criminal Code*.

253. For this reason, the amendment does not infringe on the right to a fair trial and fair hearing as protected by article 14 of the ICCPR. 'Equality of arms' requires that each party be afforded a reasonable opportunity to present their case under the conditions that do not place them at a substantial disadvantage vis-à-vis another party.[9] This principle essentially denotes equal procedural ability to state the case. This amendment does not engage the 'equality of arms' principle. This is because the amendment does not derogate from, or abridge, existing procedural rights of parties to litigation and would not result in actual disadvantage or other unfairness to the defendant. That is, the amendment does not impact upon opportunities to adduce or challenge evidence or present arguments on the matters at issue.[10]

254. Accordingly, the provisions are a reasonable and proportionate limitation on the right to a fair trial and fair hearing in article 14 of the ICCPR.

*The right to privacy under Article 17 of the ICCPR*

255. Article 17 of the ICCPR prohibits arbitrary or unlawful interference with an individual's privacy, family, home or correspondence. This right may be subject to permissible limitations where those limitations are provided by law and are non-arbitrary. In

---

[6] (1978) 141 CLR 54.
[7] Section 138 of the *Evidence Act 1995* (Cth).
[8] See s 63 of the TIA Act.
[9] *Brandstetter v Austria*, Application No: 11170/84; 12876/87; 13468/87, Strasbourg judgment 28 August 1991 §§41-69.
[10] *H. v Belgium*, Application No: 8950/80, Strasbourg judgment 30 November 1987 §§49-55.

order for limitations not to be arbitrary, they must be aimed at a legitimate objective and be reasonable, necessary and proportionate to that objective.

256. To justify a limitation of human rights, a legitimate objective must address a pressing or substantial concern and not simply seek an outcome that is desirable or convenient. The Bill is intended to enhance law enforcement agencies' abilities to prevent, detect and investigate acts of terrorism. Terrorism is a significant threat to national security and public safety for a variety of reasons. Firstly, politically motivated, violent acts can indiscriminately threaten the lives and physical safety of Australian citizens. This can perpetuate a climate of fear which is socially divisive, threatening the cohesiveness of Australian society.

257. The current threat environment has meant that terrorism has become a substantial concern for law enforcement agencies and Australian society more generally. The nature of terrorism itself is changing with smaller groups or lone actors engaging in short-term, low-complexity attack plans, reducing the warning time for attacks. From a counter-terrorism perspective, the number of persons of concern in Australia is substantially higher than at any point historically, and is expected to increase substantially if, and when, foreign fighters from the Syrian conflict return. The prevention of terrorist acts and the evolving nature of the threat justify proportionate limitations on selected human rights to support the protection of the broader community.

258. The trigger for limitations on privacy through the authorisation of interception will be the issue of a control order, issued by an independent authority in limited circumscribed circumstances. The control order regime addresses the challenge posed by terrorism and hostile activity in foreign countries by mitigating the threat posed by specific, high-risk individuals. The use of interception to monitor those subject to control orders will support monitoring of compliance with conditions imposed, and better mitigate the risk of terrorism and involvement in foreign conflicts. If a person subject to a control order perceives there is little likelihood of breaches being detected, there is little incentive for them to comply with the terms of the order, and the specific preventative effect of a control order is potentially undermined.

259. Under the current law, agencies have limited means to monitor a person's compliance with a control order, and to detect planning and preparatory acts for a terrorist act or hostile activity overseas. At present, agencies are often limited to physical surveillance, which is ineffective in many cases and is exceptionally difficult to scale due to its resource-intensive nature.

260. The amendments will allow law enforcement officers to apply to an issuing authority for a warrant for the purposes of monitoring a person subject to a control order, to prevent or protect the public from terrorism or prevent a person from assisting hostile activity in a foreign country. Consistent with the existing framework for investigative warrants, agencies will be able to apply for telecommunications service warrants (A-party and B-party) and named person warrants in strictly limited circumstances. An interception warrant may also authorise access to stored communications and telecommunications data associated with the service or device.

261. The amendments establish a number of safeguards to ensure that any interference with privacy is for a legitimate objective and implemented in a proportionate manner. Agencies are required to apply for telecommunications service, named person and B-party warrants in strictly limited circumstances. Likewise, the warrant can only be issued once a number of

thresholds are met. It is mandatory that the judge or nominated AAT member take particular circumstances into account before determining whether to issue the warrant. Agencies are not automatically entitled to receive control order warrants in relation to persons who are subject to control orders.

262. First, the judge or nominated AAT member must have regard to whether the privacy of any person would be likely to be interfered with by intercepting, under a warrant, communication made to or from the telecommunications service. The judge or AAT member must also have regard to how much the information obtained may be likely to assist in connection with:

- protecting the public from a terrorist act
- preventing the provision of support for, or the facilitation of, a terrorist act
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

263. Even where the issuing authority is satisfied that the use of telecommunications interception would be likely to assist in connection with one or more of the above purposes, the issuing authority is not required to issue a control order warrant. The decision to issue a control order monitoring warrant is discretionary, and may only be taken after the issuing authority has had regard to a range of competing public interests, including:

- how much the privacy of any person would be likely to be interfered with by interception under a warrant communications made to or from the service;
- how much the information obtained under interception would be likely to assist in connection with one or more of the above purposes;
- to what extent methods to achieve one or more of the above purposes have been used, or are available to the agency;
- how much the use of such methods would be likely to assist in connection with one or more of the above purposes;
- how much the use of such methods would be likely to prejudice an agency achieving one or more of the above purposes whether because of delay or for any other reason;
- whether interception under a warrant communications made to or from the service would be likely to have the least interference with any person's privacy; and
- the possibility that the person subject to the control order:
    - has engaged, is engaging, or will engage, in a terrorist ac
    - has provided, is providing, or will provide, support for a terrorist act
    - has facilitated, is facilitating, or will facilitate, a terrorist act
    - has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country
    - has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country

- has contravened, is contravening, or will contravene, the control order, or
- will contravene a succeeding control order.

264. The requirement to 'have regard to' the above matters requires the issuing authority to give those matters a proper, genuine and realistic consideration, and amounts to a requirement for the issuing authority to consider both the necessity for the control order warrant (including the likelihood that the person has engaged in, is engaging in, or will engage in conduct that is sought to be detected and prevented by the warrant, and the likely value of the information that is sought to be obtained, in light of any previous control order warrants issued in relation to the person) and the proportionality of issuing the control order warrant (including the likely degree of interference with the privacy of the person subject to the control order and any third parties, and the availability of alternative, less intrusive methods).

265. The issuing authority must not issue a B-Party warrant where a control order is in force in relation to another person unless he or she is satisfied that the agency has exhausted all other practicable methods, or it would not otherwise be possible to intercept a telecommunications service used or likely to be used by the person subject to the control order.

266. The Bill will enable state and territory agencies to use or communicate lawfully intercepted information in relation to their respective PDO regimes. PDOs can be used by national security and law enforcement agencies to prevent a terrorist act. Interception at the early stages of a counter-terrorism investigation can underpin applications for PDOs, which in turn can disrupt an attack.

267. The amendments also ensure that an officer or staff member of a state or territory agency who previously communicated, made use of, or made a record of lawfully intercepted information for a purpose that would now be covered by the amendment above would be taken not to have contravened the prohibition on communicating lawfully intercepted information. This will ensure that any officers who have in good faith used or communicated lawfully intercepted information for a purpose connected with state and territory PDO legislation are not liable for a breach of the TIA Act.

268. The amendments will also introduce new deferred reporting arrangements which will permit the chief officer of an agency to delay public reporting on the use of interception in relation to a control order in certain circumstances. Due to the small number of control orders which are issued, immediate reporting of any warrants for interception may enable an individual to determine whether they are the subject of interception. If a person knows, or suspects that there is an interception warrant in place, they are more likely to be able to modify their behaviour to defeat those lawful surveillance efforts. Also, if a person knows or suspects that their communications are not being monitored, the deterrence value of the control order is limited to the extent that the person believes they can engage in proscribed activity without risk of detection. Deferred reporting balances the public interest in timely and transparent reporting with the need to preserve the effectiveness of control orders to prevent individuals from committing terrorist acts.

269. The Bill will place strict controls on the decision to defer public reporting, reflecting the significant public interest in transparency in relation to the use of exceptional, covert powers. First, the decision to defer public reporting may only be made by the Minister, on

the advice of the chief officer of the relevant agency. Second, the chief officer and the Minister must each be satisfied that publicly reporting particular information could be reasonably expected to enable a reasonable person to determine that particular surveillance measures are likely to be, or not to be in force at the time he or she makes his or her decision (which will generally be at different times, given the time taken to prepare the Minister's report based on all agencies' input). Third, where public reporting is deferred in relation to particular information, the chief officer of the relevant agency will be required to reconsider his or her decision each year. Fourth, documentary records must be kept in relation to each such decision. Fifth, each such decision is subject to independent oversight by an Ombudsman.

270. The Bill allows for the limited use of either lawfully intercepted information or lawfully accessed information obtained under a warrant relating to an interim control order which is subsequently declared void. The information may be used, communicated, recorded or given in evidence in a proceeding when it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, serious damage to property or a purpose connected with a Commonwealth, state or territory PDO regime. Notwithstanding that the underlying order in relation to which the warrant was made is no longer valid, there remains a strong justification for allowing the information be used to prevent significant harm to the public. To provide otherwise would frustrate the protection of the community where communications intercepted in good faith must be relied on to prevent or reduce the commission of a terrorist act or other related serious harm.

*The right to freedom of expression in Article 19 of the ICCPR*

271. Article 19 of the ICCPR provides that all persons shall have the right to freedom of expression, including the freedom to speak, receive and impart information and ideas of all kinds, through any media of a person's choice. This right may be subject to restrictions for the purposes of national security or public order where such restrictions are provided by law and are necessary.

272. This Bill engages the right to freedom of expression indirectly, to the extent that individuals subject to control orders may suspect that their communications are being intercepted. This suspicion may cause them to restrict their communications, both in terms of content and audience. The nature of the terrorism threat is evolving, with rapid radicalisation and low sophistication attacks resulting in shorter timeframes for agencies to detect and disrupt attacks. Furthermore, returning foreign fighters will necessarily impact the domestic threat environment given their combat and tradecraft experience, and established terrorist networks. This heightened risk justifies any indirect limitation on free speech for a limited number of specific individuals subject to control orders.

*The right to an effective remedy in Article 2(3) of the ICCPR*

273. Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights or freedoms recognised by the ICCPR, including the right to have such a remedy determined by the competent judicial, administrative of legislative authorities or by any other competent authority provided for by the legal system of the State. The right to an effective remedy applies notwithstanding that a violation has been committed by persons acting in an official capacity.

274. The right to an effective remedy applies in relation to violations of other ICCPR rights and freedoms. By establishing a new control order monitoring warrant regime, the Bill indirectly creates a risk that a person's right to protection against arbitrary and unlawful interferences with privacy under Article 17 of the ICCPR may be violated where telecommunications are intercepted in connection with a control order, or information obtained under monitoring warrant is used, in a manner that is unlawful. Accordingly, the Bill engages the right to an effective remedy for any such violation of the right to privacy.

275. The Bill engages the right to an effective remedy by providing immunity, including immunity for ancillary conduct, in limited circumstances, for conduct that could otherwise found a criminal charge. The Bill protects persons from criminal liability for acts done, or omitted to be done, in good faith purportedly under the authority of the TIA Act in connection with an interim control order that has subsequently been declared to be void.

276. The scheme is necessary to ensure the effective performance of the statutory functions of law enforcement agencies, by ensuring that law enforcement officers can be confident that they will not face criminal liability for conduct engaged in in good faith:

- under a legal authority provided by the TIA Act that is valid at the time the officer engages in the conduct, or
- under a legal authority provided by the TIA Act that the officer reasonably believes to be valid at the time officer engages in the conduct.

277. Not providing this immunity would impair law enforcement agencies' capabilities and willingness to ensure a safe and secure Australia. Because a Court may declare an interim control order void *ab initio*, absent an immunity, law enforcement officers would potentially face retrospective criminal liability for conduct they engaged in, in good faith, in reliance on a legal authority that was valid at the time. The existence of such a risk would create a powerful deterrent for officers to rely on valid legal authorities.

278. The limitation to the right to an effective remedy is limited to the extent that it is reasonable, necessary and proportionate to the objective of facilitating the fulfilment of law enforcement agencies' functions in protecting the public from acts of terrorism, preventing the engagement in hostile activities in foreign countries, and monitoring persons' compliance with control orders. The immunity is limited to conduct engaged in, in good faith, and does not apply if, at that time, the person knew, or ought reasonably to have known, that the interim control order underpinning the legal authority provided by the TIA Act had been declared void. In particular, the Bill also does not immunise law enforcement agencies (which would ordinarily assume vicarious liability for acts done or omitted to be done by their officers) from civil liability for any such conduct; persons may therefore seek civil remedies for damage or harm suffered as a result of any act done, or omitted to be done, under the authority of the TIA Act where that authority was dependent upon the existence of an interim control order that has subsequently been declared void.

279. The Bill and TIA Act otherwise protect the right to an effective remedy. Unlawful interception of, and access to, a communication, and unlawful uses of lawfully intercepted or accessed information, are criminal offences punishable by up to two years' imprisonment. Individuals may also apply to a court for a civil remedy if they suspect that their communications have been unlawfully intercepted or accessed.

**Conclusion**

280. While the Bill engages a range of human rights, it is compatible with human rights because it promotes some rights, and to the extent that it limits some rights, those limitations are reasonable, necessary and proportionate in achieving a legitimate objective.

**NOTES ON CLAUSES**

**Clause 1 – Short title**

282. Clause 1 provides for the short title of the Act to be the *Counter-Terrorism Legislation Amendment Act (No. 1) 2016*.

**Clause 2 – Commencement**

283. This clause provides for the commencement of each provision in the Bill, as set out in the table.

284. The table in subclause 2(1) provides that all the provisions in each of the Schedules commence on the day the Act receives Royal Assent, except for Part 2 of Schedule 15. Part 2 of Schedule 15 will commence on a single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 12 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period. The note to subclause 2(1) clarifies that the table only relates to the provisions of this Act as enacted, and not to later amendments to those provisions.

285. Subclause 2(2) provides that information in column 3 of the table is not part of the Act. It is designed to assist readers, and may be updated or changed in any published version of this Act.

**Clause 3 – Schedules**

286. Each Act specified in a Schedule to this Act is amended as is set out in the applicable items in the Schedule. Any other item in a Schedule to this Act has effect according to its terms.

**Schedule 1—Receiving funds for legal assistance**

***Criminal Code Act 1995***

**Item 1 – After paragraph 102.6(3)(a)**

288. This item inserts new paragraph 102.6(3)(aa) after paragraph 102.6(3)(a).

289. Currently, subsections 102.6(1) and (2) of the *Criminal Code* criminalise receiving funds from, making funds available to, or collecting funds for a terrorist organisation. The difference between the two provisions is that subsection 102.6(1) deals with the situation where the offender knows the organisation is a terrorist organisation, and subsection 102.6(2) deals with the situation where the offender is reckless as to whether the organisation is a terrorist organisation. Subsection 102.6(1) carries a maximum penalty of 25 years imprisonment and subsection 102.6(2) carries a maximum penalty of 15 years imprisonment.

290. 'Terrorist organisation' is defined in section 102.1 of the *Criminal Code*. 'Funds' are broadly defined in section 100.1 of the *Criminal Code*, and cover property and assets of every kind.

291. Currently, paragraph 102.6(3)(a) of the *Criminal Code* provides the offence does not apply to a person who receives funds from the organisation if the person proves that he or she received the funds solely for the purpose of the provision of legal representation for a person in proceedings relating to Division 102. For example, a lawyer is able to receive funds from a terrorist organisation if it is for the purpose of representing a person in a prosecution for a terrorist organisation offence under Division 102. In addition, paragraph 102.6(3)(b) provides the offence does not apply where the person receives the funds solely for the purpose of providing assistance to the organisation for it to comply with a law of the Commonwealth or a state or territory.

292. Recommendation 20 of the COAG Review was that the exception in paragraph 102.6(3)(a) should be broadened and include similar exemptions to those for the offence of associating with a terrorist organisation in paragraph 102.8(4)(d) of the *Criminal Code*. COAG supported this recommendation, in part, and considered that to the extent that subparagraph 102.8(4)(d)(ii) exempts the provision of legal assistance in matters involving the question of whether an entity is a terrorist organisation, it is appropriate that an exemption along these lines is incorporated in paragraph 102.6(3)(a).

293. This item implements that response and inserts new paragraph 102.6(3)(aa) so that, in addition to the existing exceptions, the offence does not apply where a lawyer receives funds from an organisation for the purpose of providing legal advice in connection with the question of whether the organisation is a terrorist organisation. Paragraph 102.6(3)(aa) is not restricted to proceedings relating to Division 102.

294. It is appropriate that an organisation is provided with an opportunity to contest a determination that it is a terrorist organisation. The amendment will enable a lawyer to receive funds from a terrorist organisation in cases where it seeks to challenge its status as a terrorist organisation. However, the exception will not extend to receiving funds for legal services that could help the organisation flourish. For example, lawyers will not be able to receive funds for providing legal advice or legal representation in general commercial or civil transactional matters.

295. As with the existing exception to subsection 102.6(3), a defendant bears the legal burden to prove the exception under paragraph 102.6(3)(aa).

**Item 2 – Subparagraph 102.8(4)(d)(ii)**

296. This item amends subparagraph 102.8(4)(d)(ii).

297. Section 102.8 of the *Criminal Code* criminalises associating with individuals who are members of, or promote or direct the activities of a terrorist organisation. Currently, subparagraph 102.8(4)(d)(ii) provides an exception to the offence where the association is only for the purpose of providing legal advice or legal representation in connection with 'proceedings relating to whether the organisation in question is a terrorist organisation'.

298. Proposed subparagraph 102.8(4)(d)(ii) removes the reference to 'proceedings'. Currently, the reference to proceedings in subparagraph 102.8(4)(d)(ii) could create uncertainty as to whether formal proceedings must be instituted before the exemption applies. The amendment removes this ambiguity and provides certainty that legal advice or legal representation can be provided in relation to the question of whether the organisation in question is a terrorist organisation, before proceedings are formally instituted or have commenced.

## Schedule 2—Control orders for young people

### *Criminal Code Act 1995*

### Overview

300. Control orders under Division 104 of Part 5.3 of the *Criminal Code* can currently be made only in relation to persons 16 years of age or older and a control order can only be made in relation to a young person aged 16 or 17 for a maximum duration of three months, rather than the maximum of 12 months applicable for persons over the age of 18.

301. These amendments will allow control orders to be imposed on a young person who is 14 or 15 years of age. This age threshold is higher than the age at which a young person can be prosecuted for a criminal offence in Australia (ten years of age). As with existing control orders made in relation to a young person aged 16 or 17, a control order will only be able to be made in relation to a young person aged 14 or 15 for a maximum duration of three months.

302. These amendments respond to incidents in Australia and overseas that demonstrate persons as young as 14 years of age are organising and participating in terrorism related conduct. With school-age students being radicalised and engaging in radicalising others and capable of participating in activity that poses a threat to national security, the age limit of 16 years is no longer sufficient if control orders are to be effective in preventing terrorist activity.

### Item 1 – Paragraph 104.2(3)(b) of the *Criminal Code*

303. This item repeals existing paragraph 104.2(3)(b) of the *Criminal Code* and replaces it with new paragraphs 104.2(3)(b) and (ba).

304. Currently, paragraph 104.2(3)(b) provides that, if a senior AFP member is seeking the Attorney-General's consent for an interim control order in relation to a person, and the senior AFP member has information about the person's age (regardless of the person's age), he or she must give that information to the Attorney-General.

305. New paragraphs 104.2(3)(b) and (ba) provide for different requirements depending on the age of the proposed subject of the control order.

306. Specifically, paragraph 104.2(3)(b) provides that, if a senior AFP member is seeking the Attorney-General's consent for an interim control order in relation to a person who is at least 18 years of age and the senior AFP member has information about the person's age, he or she must give that information to the Attorney-General. This paragraph does not place any additional burden on the senior AFP member to obtain information about the proposed subject's age.

307. In contrast, paragraph 104.2(3)(ba) provides that, if a senior AFP member is seeking the Attorney-General's consent for an interim control order in relation to a person who is under 18 years of age, the senior AFP member must give information about the young person's age to the Attorney-General. This places an obligation on the senior AFP member to obtain information about the proposed subject's age before seeking the Attorney-General's consent to apply for a control order in relation to a young person.

**Item 2 – Subsection 104.2(3) of the *Criminal Code* (note)**

308. This item is consequential to the amendment to subsection 104.28(1) which provides that a control order may not be issued to a person under the age of 14 years. This item amends the note immediately following subsection 104.2(3) by replacing '16' with '14', and advises readers that a senior AFP member cannot request the Attorney-General's consent to apply for a control order in relation to a person who is under 14 years of age (see section 104.28).

**Item 3 – Paragraph 104.4(2) of the *Criminal Code***

309. This item replaces the existing requirement in subsection 104.4(2) for an issuing court to take into account the impact of each control on the person's circumstances (including the person's financial and personal circumstances) in determining whether each control to be imposed on the person by the order is reasonably necessary, and reasonably appropriate and adapted to one of the purposes set out in the Division.

310. New paragraph 104.4(2)(a) requires the issuing court to take into account as a 'paramount consideration' the objects of the Division (see section 104.1) in all cases when determining whether each of the controls to be imposed on the person by the control order is reasonably necessary, and reasonably appropriate and adapted.

311. New paragraph 104.4(2)(b) requires the issuing court to take into account as a 'primary consideration' 'the best interests' of the person when considering whether to impose each of the controls on a young person aged 14 to 17 years. The requirement for the court to consider the best interests of the person aged from 14 to 17 years is consistent with Article 3 of the CRC and is adapted from the Family Law Act.

312. The existing obligation for an issuing court to take into account the impact of each control on the person's circumstances (including the person's financial and personal circumstances) is moved to new paragraph 104.4(2)(c) and applies as an 'additional consideration' in relation to all potential subjects of a control order.

313. This amendment will ensure that, in determining whether each of the controls to be imposed on a person by the interim control order is reasonably necessary, and reasonably appropriate and adapted, the issuing court must give appropriate weight to each of the considerations. The terms 'paramount consideration', 'primary consideration', and 'additional consideration' are drawn from the Family Law Act and operate to distinguish the weight given to consideration of the requirements in each paragraph.

314. New subsection 104.4(2A) provides guidance for the issuing court when considering the best interests of the young person under paragraph 104.4(2)(b). Specifically, the matters the court must take into account include, but are not limited to:

- the young person's age, maturity, sex and background (including lifestyle, culture and traditions)
- the young person's physical and mental health
- the benefit to the young person of having a meaningful relationship with his or her family and friends
- the right of the young person to receive an education

- the right of the young person to practice his or her religion, and
- any other matter the issuing court considers relevant.

315. This list is adapted from the Family Law Act and is consistent with Australia's international obligations under Article 3 of the CRC.

**Item 4 – Subsection 104.5(1) of the *Criminal Code* (note 2)**

316. This item repeals and replaces note 2 after subsection 104.5(1). The new note advises that the maximum duration of a confirmed control order in relation to a young person is three months after the day on which the interim control order was made (see section 104.28).

**Item 5 – After subparagraph 104.12(1)(b)(iii) of the *Criminal Code***

317. This item inserts new subparagraph 104.12(1)(b)(iiia) after existing subparagraph 104.12(1)(b)(iii).

318. Subsection 104.12(1) currently requires an AFP member to serve the control order personally on the subject and to inform the person of certain matters. New subparagraph 104.12(1)(b)(iiia) will also require the AFP member to inform the subject of the right to obtain legal advice and legal representation. Nothing in existing Division 104 precludes an individual, young person or otherwise, from seeking legal advice and legal representation. However, this amendment ensures that all persons, regardless of age, are informed of this right in relation to control order proceedings.

319. The terms 'legal advice' and 'legal representation' have been used to allow the provisions to apply flexibly and enable a subject to engage legal representation as they consider appropriate.

320. This item implements Recommendation 2 of the Committee advisory report. The advisory report recommended the removal of the role of the court appointed advocate in relation to control order proceedings for young persons and suggested a more effective and appropriate safeguard is to ensure the right of the young person to legal representation. The amendment implements the recommendation and extends the requirements to all potential subjects of a control order, not just young persons aged 14 to 17 years.

**Item 6 – Subsection 104.12(5) of the *Criminal Code* (heading)**

321. This item repeals the heading 'Queensland public interest monitor to be given copy of interim control order' and replaces it with the simpler, more succinct heading 'If person is resident, or order made, in Queensland'.

**Item 7 – At the end of section 104.12 of the *Criminal Code***

322. This item inserts a new heading 'If person is 14 to 17' at the end of section 104.12.

323. This item also inserts a new subsection 104.12(6) after the new heading.

324. New subsection 104.12(6) provides that, as soon as practicable after an interim control order is made in relation to a person aged 14 to 17 years, and at least 48 hours before the day specified in the order for the confirmation hearing, an AFP member must take

reasonable steps to personally serve a copy of the order on at least one parent or guardian of the person. The term 'reasonable' is to be given its ordinary meaning and will be determined at the time of service or attempted service.

325. There will be instances where it is not possible to identify and/or locate a parent or guardian. For example, the young person could be estranged from his or her parents or guardians, or those individuals could be overseas or otherwise unable to be contacted. 'Reasonable steps' also acknowledges that the young person may not cooperate with authorities in seeking to identify his or her parents or guardians. It is fundamental that an inability to serve one of the young person's parents or guardians with the order does not frustrate the commencement of the order.

326. If the AFP member has taken reasonable steps to personally serve a copy of the order on at least one parent or guardian of the young person, but service was not successful, the AFP member is not required to attempt to personally serve a copy of the order on another parent or guardian. However, the amendments do not prevent the AFP member from doing so.

327. Service in some other contexts involving young persons, such as under the Family Law Act, includes a positive requirement to serve the parent or guardian. However, in those circumstances the parent or guardian is a party to the proceedings and has a clear interest in receiving all relevant documents. In the case of a control order the parent or guardian is not a party to the proceedings.

**Item 8 – Subparagraph 104.12A(2)(a)(iii) of the *Criminal Code***

328. This item makes a technical amendment to subparagraph 104.12A(2)(a)(iii). Paragraph 104.12A(2)(a) currently provides that, where a senior AFP member elects to confirm an interim control order he or she must personally serve certain things on the person in relation to whom the order is made. This currently includes a requirement to provide any 'other' details.

329. The amendment clarifies that the requirement is to provide any other 'written' details, acknowledging that it would be unnecessarily burdensome to require the AFP to provide details that are not in written form.

**Item 9 – At the end of subsection 104.12A(2) of the *Criminal Code***

330. This item adds a new paragraph 104.12A(2)(c) at the end of existing subsection 104.12A(2).

331. New paragraph 104.12A(2)(c) provides that, if the subject of the control order is aged 14 to 17 years, prior to the day specified in the order for the confirmation hearing, an AFP member must take reasonable steps to personally serve a copy of the written notification of the decision to confirm the order and all other documents required to be served on the person the subject of the control order, on at least one parent or guardian of the person. The term 'reasonable' is to be given its ordinary meaning and will be determined at the time of service or attempted service.

332. The amendment is intended to operate flexibly to allow the AFP member to serve, or attempt to serve, on a parent or guardian of the young person, irrespective of whether it is the

same parent or guardian who was served a copy of the initial order. This acknowledges that there will be instances where, even though the young person's parents or guardians were able to be identified and located for the purposes of serving the initial order, it may not be possible or practicable to locate the same parent or guardian at this subsequent stage. It also reflects the fact that parents and guardians are not parties to the control order proceedings. It is fundamental that an inability to serve one of the young person's parents or guardians with the relevant documents does not prevent confirmation of the order.

333. If the AFP member has taken reasonable steps to personally serve a copy of the order on at least one parent or guardian of the young person, but service was not successful, the AFP member is not required to attempt to personally serve a copy of the order on another parent or guardian. However, the amendments do not prevent the AFP member from doing so.

**Item 10 – At the end of subsection 104.12A(4)(b) of the *Criminal Code***

334. This item inserts new subparagraph 104.12A(4)(iv).

335. Existing subsection 104.12A(4) sets out the requirements where the AFP senior member elects not to confirm an interim control order that has been served on a person.

336. Where the subject of the interim control order is 14 to 17 years of age, new subparagraph 104.12A(4)(b)(iv) requires the AFP member to cause reasonable steps to be taken to serve a copy of the annotated order and the notification personally on at least one parent or guardian of the young person.

337. This amendment is designed to ensure a parent or guardian of the young person is informed that the interim control order has ceased to be in force and can take appropriate steps to provide information about the consequences of that fact to the young person.

338. The term 'reasonable' is to be given its ordinary meaning and will be determined at the time the action is taken. The amendment is intended to operate flexibly to allow service on a parent or guardian of the young person, irrespective of whether it is the same parent or guardian who has previously been served orders or documents in relation to the control order proceedings.

**Item 11 – Before subsection 104.14(1) of the *Criminal Code***

339. This item inserts a new heading and subsection into existing section 104.14.

340. Existing section 104.14 sets out the steps for confirming an interim control order, including adducing evidence or making submissions, attendance at court and failure of a person or representative to attend court.

341. New heading 'When this section applies' and new subsection 104.14(1A) are inserted before existing section 104.14(1). New subsection 104.14(1A) is designed to ensure an interim control order cannot be confirmed by an issuing court unless all legislative requirements in relation to service, explanation, notification, election and annotation have been complied with.

342. New subsection 104.14(1A) clarifies that existing section 104.14 only applies where the three criteria set out in new paragraphs 104.14(1A)(a) to (c) are met. Those criteria are

that an interim control order has been made in relation to a person (paragraph 104.14(1A)(a)), the AFP has elected to confirm the order (paragraph 104.14(1A)(b)), and the issuing court is satisfied on the balance of probabilities that all requirements in section 104.12 relating to service, explanation and notification of the interim control order, as well as all requirements in section 104.12A relating to election, annotation, notification and service have been complied with (paragraph 104.14(1A)(c)).

**Item 12 – Subsection 104.14(1) of the *Criminal Code***

343. This item omits the words 'If an election has been made to confirm an interim control order, then, on' and replaces them with 'On'. This item is consequential to the amendments to new subsection 104.14(1A).

**Item 13 – Paragraph 104.14(1)(e) of the *Criminal Code***

344. This item is a technical amendment which omits the words '(unless the monitor is already a representative of the person)' from existing paragraph 104.14(1)(e), on the basis that the words are unnecessary.

**Item 14 – Subsection 104.14(4) of the *Criminal Code***

345. This item repeals and replaces the text of existing subsection 104.14(4) which applies where no-one attends court to adduce evidence or make representations in relation to the confirmation of the order.

346. Revised subsection 104.14(4) provides that the court may confirm the interim control order without variation if neither the subject of the control order, a representative of the subject, nor the Queensland public interest monitor (if relevant) attend the court on the specified day.

347. The previous provision in subsection 104.14(4), that the court must be satisfied that the order was properly served on the person, is replaced by revised subsection 104.14(1A), which requires that before confirming an interim control the court must be satisfied that the requirements in sections in 104.12 and 104.12A have been complied with.

**Item 15– Subsection 104.16(1) of the *Criminal Code* (note)**

348. This item repeals and replaces the note to subsection 104.16. The new note advises that the maximum duration of a confirmed control order in relation to a young person is three months after the day on which the interim control order was made (see section 104.28).

**Item 16 – At the end of section 104.17 of the *Criminal Code***

349. This item adds a new heading 'If person is 14 to 17' and a new subsection 104.17(4) to existing section 104.17.

350. Existing section 104.17(1) sets out the requirements in relation to service of a declaration, revocation, variation or confirmation of an interim control order.

351. New subsection 104.17(4) provides that, as soon as practicable after an interim control order in relation to a person aged 14 to 17 years is declared to be void, revoked or confirmed, an AFP member must take reasonable steps to serve a copy of the declaration,

revocation or confirmed control order personally on at least one parent or guardian of the young person.

**Item 17 – Paragraph 104.18(4)(e) of the *Criminal Code***

352. This item is a technical amendment which omits the words '(unless the monitor is already a representative of the person)' from existing paragraph 104.18(4)(e). Those words are unnecessary.

**Item 18 – After subsection 104.19(2) of the *Criminal Code***

353. This item inserts new subsection 104.19(2A).

354. Existing subsection 104.19(2) specifies the individuals who must be notified of the application and grounds for the application where the AFP Commissioner applies to revoke or vary an order.

355. New subsection 104.19(2A) provides that, where the subject of the control order is aged from 14 to 17 years, the AFP Commissioner must cause reasonable steps to be taken to give written notice of both the application and the grounds on which the revocation or variation is sought to at least one parent or guardian of the person.

**Item 19 – Paragraph 104.19(3)(e) of the *Criminal Code***

356. This item is a technical amendment which omits the words '(unless the monitor is already a representative of the person)' from paragraph 104.19(3)(e), on the basis that these words are unnecessary.

**Item 20 – Subsection 104.20(3) of the *Criminal Code***

357. This item repeals and replaces existing subsection 104.20(3).

358. Existing subsection 104.20(3) requires an AFP member to serve a revocation or variation of a confirmed control order on the subject of the control order as soon as practicable after the order is revoked or varied.

359. New paragraph 104.20(3)(a) replicates that requirement.

360. Where the subject of the control order is aged 14 to 17 years, new paragraph 104.20(3)(b) also requires the AFP member to take reasonable steps to serve a copy of the revocation or variation personally on at least one parent or guardian of the person.

**Item 21 – Paragraph 104.23(2)(d) of the *Criminal Code***

361. This item repeals and replaces existing paragraph 104.23(2)(d) and inserts new paragraph 104.23(2)(e).

362. Existing subsection 104.23(2) sets out the obligations imposed on the AFP Commissioner when he or she applies to an issuing court to add one or more obligation, prohibitions or restrictions to a confirmed control order.

363. New paragraph 104.23(2)(d) replicates existing paragraph 104.23(2)(d) by requiring the AFP Commissioner to provide information about the person's age, if known.

364. Where the subject of the confirmed control order is aged 14 to 17 years, new paragraph 104.23(2)(e) imposes a positive obligation on the AFP Commissioner to give the issuing court information about the young person's age.

**Item 22 – Subsection 104.23(2) of the *Criminal Code* (note 1)**

365. This item amends note 1 immediately following subsection 104.23(2), and is consequential to the amendment to subsection 104.28 which provides that a control order may not be issued to a person under 14, rather than under 16, years of age.

366. New note 1 advises that a control order may not be requested in relation to a person who is under 14 years of age (see section 104.28).

**Item 23 – Subsection 104.23(3) of the *Criminal Code***

367. This item repeals and replaces existing subsection 104.23(3) and inserts new subsection 104.23(3AA).

368. Existing subsection 104.23(3) sets out the obligations imposed on the AFP Commissioner when applying to vary a confirmed control order by adding one or more obligations, prohibitions or restrictions.

369. As soon as practicable after an application is made, new subsection 104.23(3) requires the Commissioner to cause documents mentioned in new subsection 104.23(3AA) to be served personally on the person subject to the order (paragraph 104.23(3)(a)) and the Queensland public interest monitor (if relevant) (paragraph 104.23(3)(b)). Additionally, if the person is 14 to 17 of age the Commissioner must cause reasonable steps to be taken to serve the documents mentioned in new subsection 104.23(3AA) personally on at least one parent or guardian of the person.

370. New subsection 104.23(3AA) provides that the documents referred to in subsection 104.23(3) are:

- the written notice of the application and the grounds on which the variation is sought
- a copy of the documents that explain why each obligation, prohibition and restriction should be imposed and any facts relating to why they should not be imposed, and
- any other written details required to enable the subject of the control order to understand and respond to the substance of the facts, matters and circumstances which will form the basis of the variation of the order.

**Item 24 – Subsection 104.23(3A) of the *Criminal Code***

371. This item omits the words 'subsection (3) does' and replaces them with 'subsections (3) and (3AA) do'. This amendment is consequential to the revision of subsection 104.23(3) and the insertion of new subsection 104.23(3AA).

**Item 25 – Paragraph 104.23(4)(e) of the *Criminal Code***

372. This item is a technical amendment that omits the words in brackets, '(unless the monitor is already a representative of the person)' from paragraph 104.23(4)(e), on the basis that these words are unnecessary.

**Item 26 – Subsection 104.24(2) of the *Criminal Code***

373. This item repeals and replaces existing subsection 104.24(2) and inserts a new subsection 104.24(2A).

374. This item replaces the existing requirement in subsection 104.24(2) for an issuing court to take into account the impact of the obligation, prohibition or restriction on the person's circumstances (including the person's financial and personal circumstances) in determining whether each of the obligations, prohibitions and restrictions to be imposed on the person by the order are reasonably necessary, and reasonably appropriate and adapted.

375. New paragraph 104.24(2)(a) requires the issuing court to take into account as a 'paramount consideration' the objects of Division 104 in all cases when determining whether each of the obligations, prohibitions and restrictions to be imposed on the person by the order is reasonably necessary, and reasonably appropriate and adapted.

376. New paragraph 104.24(2)(b) requires the issuing court to take into account as a 'primary consideration' 'the best interests' of the person when considering whether to impose each of the obligations, prohibitions and restrictions on a young person aged 14 to 17 years.

377. The existing obligation for an issuing court to take into account the impact of the obligation, prohibition or restriction on the person's circumstances (including the person's financial and personal circumstances) is moved to new paragraph 104.24(2)(c) and applies as an 'additional consideration' in relation to all potential subjects of a control order.

378. This amendment will ensure that, in determining whether each of the obligations, prohibitions and restrictions to be imposed on a person by variation of a control order is reasonably necessary, and reasonably appropriate and adapted, the issuing court must give appropriate weight to each of the considerations. The terms 'paramount consideration', 'primary consideration', and 'additional consideration' are drawn from the Family Law Act and operate to distinguish the weight given to consideration of the requirements in each paragraph.

379. New subsection 104.24(2A) provides guidance for the issuing court when considering the best interests of the young person under paragraph 104.24(2)(b). The matters the court must take into account are listed in new subsection 104.2(2A). The matters include, but are not limited to:

- the young person's age, maturity, sex and background (including lifestyle, culture and traditions)
- the young person's physical and mental health
- the benefit to the young person of having a meaningful relationship with his or her family and friends
- the right of the young person to receive an education

- the right of the young person to practice his or her religion, and
- any other matter the issuing court considers relevant.

380. This list is adapted from the Family Law Act and is consistent with Australia's international obligations under Article 3 of the CRC.

**Item 27 – At the end of section 104.26 of the *Criminal Code***

381. This item inserts a new heading 'If person is 14 to 17 years' and a new subsection 104.26(5).

382. Existing section 104.26 sets out the requirement in relation to service and explanation of a varied control order.

383. New subsection 104.26(5) sets out the additional requirements where the subject of the control order is aged 14 to 17 years. Specifically, as soon as practicable after a control order in relation to a young person is varied under section 104.24, an AFP member must take reasonable steps to serve a copy of the varied order personally on at least one parent or guardian of the young person.

**Item 28 – Subdivision H of Division 104 of Part 5.3 of the *Criminal Code* (heading)**

384. This item makes a technical amendment by repealing the existing heading, 'Subdivision H—Miscellaneous' and replacing it with a new heading 'Subdivision H—Special rules for young people (14 to 17)'.

**Item 29 – Subsection 104.28(1) of the *Criminal Code* (heading)**

385. This item makes a technical amendment by repealing the existing heading, 'Rule for persons under 16' and replaces it with a new heading 'Rule for people under 14'. This amendment reflects the reduction in the minimum age for the imposition of a control order from 16 to 14.

**Item 30 – Subsection 104.28(1) of the *Criminal Code***

386. This item amends existing subsection 104.28(1) by replacing the reference to '16' with '14'.

387. Existing subsection 104.28(1) specifies that a control order cannot be imposed on a person under 16 years of age.

388. Revised subsection 104.28(1) provides that a control order cannot be imposed on a person under 14 years of age.

**Item 31 – Subsection 104.28(2) of the *Criminal Code* (heading)**

389. This item makes a technical amendment by repealing the existing heading, 'Rule for persons who are at least 16 but under 18' and replaces it with a new heading 'Rule for people 14 to 17'. This amendment reflects the reduction in the minimum age for the imposition of a control order from 16 to 14.

**Item 32 – Subsection 104.28(2) of the *Criminal Code***

390. This item amends subsection 104.28(2) by replacing the words 'at least 16 but under 18' with the words '14 to 17 years of age'.

391. Revised subsection 104.28(2) provides that an issuing court can only issue a control order in relation to a person who is aged 14 to 17 years for a maximum duration of three months after the day on which the interim control order is made by the court.

**Item 33 – Before section 104.28A of the *Criminal Code***

392. This item inserts a new heading 'Subdivision I—Miscellaneous' before section 104.28A.

**Item 34 – At the end of subsection 104.29(2) of the *Criminal Code***

393. This item inserts new paragraph 104.29(2)(j).

394. Existing section 104.29 sets out the annual reporting obligations imposed on the Attorney-General in relation to control orders. Specifically, each year the Attorney-General is required to prepare and table a report, including the following matters with respect to control orders:

- the number of interim control orders made
- the number of interim control orders the AFP elected not to confirm
- the number of interim control orders confirmed
- the number of control orders declared void
- the number of control orders revoked
- the number of control orders varied, and
- particulars of complaints and 'AFP conduct or practices issues'.

395. New paragraph 104.29(2)(g) will require the Attorney-General to separately include information in each annual report in relation to each of the above matters concerning persons aged 14 to 17 years.

**Schedule 3—Control orders and tracking devices**

***Criminal Code Act 1995***

**Overview**

397. Division 104 of Part 5.3 of the *Criminal Code* empowers an issuing court to impose a requirement that a person subject to a control order wear a tracking device. These amendments provide that where an issuing court imposes such a requirement as part of a control order, the court must also:

- authorise the AFP to take steps specified in the control order to ensure the tracking device and associated equipment remain operational and functional
- authorise the AFP to enter premises to install equipment necessary for the operation of the tracking device, and
- impose obligations on the subject of the control order to ensure the tracking device remains operational and functional.

398. These amendments also create offences for interfering with the operation of a tracking device. These amendments respond to concerns that, if no such obligations or prohibitions are imposed, the subject of the control order or another person could allow the battery of the device to run flat or could damage the device, making it ineffective.

**Item 1 – After subsection 104.5(3) of the *Criminal Code***

399. This item inserts new subsections 104.5(3A) and 104.5(3B) after subsection 104.5(3).

400. New subsection 104.5(3A) provides that when an issuing court makes an interim control order imposing a requirement on a person to wear a tracking device under paragraph 104.5(3)(d), the court must also impose ancillary requirements on the person that ensure the proper operation of the tracking device.

401. The requirements and authorisations in new subsections 104.5(3A) and 104.5(3B) will only apply to an individual subject to a control order where the terms of that control order include a requirement to wear a tracking device under paragraph 104.5(3)(d).

402. Control orders supplement traditional law enforcement actions such as arrest and criminal prosecution as short to medium-term measures to manage and mitigate the risks posed by a person and protect the public from the serious harm and societal impact of a terrorist attack. The additional requirements and authorisations are designed to ensure the utility of a requirement to wear a tracking device in achieving these objectives.

403. New subsection 104.5(3A) provides that when an issuing court makes an interim control order imposing a requirement on a person to wear a tracking device under paragraph 104.5(3)(d), the court must also impose ancillary requirements on the person that ensure the proper operation of the tracking device.

404. The existing control order regime does not require that a person required to wear a tracking device must ensure the tracking device is charged and operational. Requiring the subject of a control order to take steps to ensure that the device is charged and operational is

necessary to prevent the person frustrating the effective operation of the requirement without technically breaching the requirements of the control order, which carries a criminal penalty. Ensuring the effective operation of a requirement to wear a tracking device is designed to support compliance with other related conditions, such as restrictions on movement and curfews.

405. New paragraph 104.5(3A)(a) requires the subject of the control order to take steps specified in the order and reasonable steps to ensure that the tracking device and any equipment necessary for the operation of the tracking device are or remain in good working order.

406. 'Steps specified in the order' are approved by the issuing court and are known to the subject of the control order at the time the control order is made. Steps specified in the order are likely to be steps which are known by the AFP as supporting the effective operation of a tracking device. Steps specified in the order may include such things as charging the tracking device for a specified time period at specified intervals.

407. The term 'reasonable steps' at paragraph 104.5(3A)(a) is included to ensure flexibility in the operation of these provisions, including where a novel situation may arise. The term 'reasonable' is to be given its ordinary meaning and will be determined at the time the situation arises. Examples of reasonable steps include but are not limited to:

- notifying the AFP if the device becomes too loose to wear
- allowing an AFP member to inspect the tracking device where warranted by the circumstances (where the situation is not covered by specified steps in the order), and
- notifying the AFP if the tracking device or associated equipment emits uncommon sounds or signals.

408. New paragraph 104.5(3A)(b) requires the subject of the control order to report at specified times and places, to persons specified in the order, for the purposes of having the tracking device inspected. This requirement, which is similar to a bail reporting condition, would facilitate inspection of the tracking device by the AFP to ensure the continued operation of the tracking device. This requirement is designed to balance the person's privacy against the need to ensure a tracking device remains operational and ensures that a person's compliance with certain terms of a control order can be examined only at specified times, unless otherwise reasonable in the circumstances.

409. New paragraph 104.5(3A)(c) requires the subject of the control order to notify an AFP member as soon as practicable, and not later than four hours after, becoming aware that the tracking device or any equipment necessary for the operation of the tracking device are not in good working order. This obligation is designed to ensure proactive communication between the subject and the AFP and will allow situations where the device is not operating properly to be dealt with in a more reasonable manner that takes into account the subject's situation at the time.

410. New subsection 104.5(3B) provides that when an issuing court makes an interim control order imposing a requirement on a person to wear a tracking device under paragraph 104.5(3)(d), the court must also authorise the AFP to take ancillary actions that ensure the proper operation of the tracking device.

411. New paragraph 104.5(3B)(a) provides that the court must authorise the AFP to take steps specified in the order to ensure that the tracking device and any equipment necessary for the operation of the tracking device are or remain in good working order. The term 'steps specified in the order' is identical to that set out in paragraph 104.5(3A)(a) and is to be interpreted and applied as outlined above.

412. New paragraph 104.5(3A)(b) provides that the court must authorise the AFP to enter specified premises to install equipment necessary for the operation of the tracking device. The provision authorises access to one or more premises as the person the subject of the order may work or reside at multiple locations, and the installation of multiple sets of equipment would facilitate monitoring of the subject's compliance with conditions of the control order.

**Item 2 – Subdivision G of Division 104 of Part 5.3 of the *Criminal Code* (heading)**

413. This item makes a technical amendment by repealing the existing heading, 'Subdivision G—Contravening a control order' and replacing it with a new heading 'Subdivision G—Offences relating to control orders'. This amendment reflects the insertion of offences in relation to tracking devices which do not constitute contravention of a control order by the subject, but constitute an offence by a third party.

**Item 3 – At the end of Subdivision G of Division 104 of Part 5.3 of the *Criminal Code***

414. This item inserts new section 104.27A after section 104.27.

415. New subsection 104.27A(1) makes it an offence for the subject of a control order to engage in conduct which results in the interference with, disruption or loss of, a function of the tracking device. The offence carries a maximum penalty of imprisonment for five years.

416. New subsection 104.27A(2) makes it an offence for a person, other than the subject of a control order, to engage in conduct which results in the interference with, disruption or loss of, a function of the tracking device. The person must either know or be reckless as to whether a control order is in force in relation to the other person. The offence carries a maximum penalty of imprisonment for five years.

417. The term 'engage in conduct' is defined in subsection 4.1(1) of the *Criminal Code* and includes acts and omissions. Conduct may range from a subject failing to charge a tracking device where there has been adequate warning that the device requires charging, to attempting to disable the tracking device by administering blunt force.

418. The creation of specific offences in relation to the requirement to wear a tracking device supplements the existing general offence for contravening a control order which is contained in section 104.27. The creation of specific offence provisions in relation to tracking devices does not prevent the application of the general offence provision in section 104.27 to a person's contravention of the requirement to wear a tracking device, and any ancillary requirements. The AFP will lay charges that are most appropriate to the circumstances of a particular case. The specific offences are intended to ensure that there are no unforseen gaps in capturing the full range of actions or inactions which may render a tracking device inoperative, and therefore undermine its efficacy.

419. The maximum penalty of imprisonment for five years is identical to the penalty applied to the offence of contravening a control order in section 104.27. Parity of these

penalties is appropriate given that all of the offences are directed to similar sorts of wrongdoing that frustrate and undermine the efficacy of the control order regime.

420. This item implements part of Recommendation 8 of the Committee advisory report that there be a clear prohibition on interfering with a tracking device.

421. Any prosecution for an offence must be supported by admissible evidence and both the physical and fault elements proved to the criminal standard beyond reasonable doubt.

**Schedule 4—Issuing court for control orders**

***Criminal Code Act 1995***

**Item 1 – Subsection 100.1(1) of the *Criminal Code* (paragraph (b) of the definition of issuing court)**

422. This item removes the Family Court of Australia from the definition of 'issuing court' in section 100.1 of the *Criminal Code*. The Federal Court of Australia and the Federal Circuit Court of Australia will be the only issuing courts for the purposes of Part 5.3 of the *Criminal Code*.

423. An issuing court has the power to make various orders under Part 5.3, including issuing, revoking and specifying the terms of a control order. While the Federal Court and the Federal Circuit Court both exercise various functions relevant to criminal law and counter-terrorism as part of their normal jurisdiction, the Family Court does not otherwise exercise functions in relation to those matters. Given its other areas of jurisdiction, it is anomalous for the Family Court to play a role in the control order regime, and the primary purpose of this amendment is to remove that anomaly.

**Schedule 5—Preventative detention orders**

***Criminal Code Act 1995***

**Overview**

424. The purpose of the PDO regime in Division 105 of the *Criminal Code* is to allow a person to be taken into custody and detained for a short period of time, being no longer than 48 hours under the Commonwealth regime, in order to prevent an imminent terrorist act occurring, or to preserve evidence of, or relating to, a recent terrorist act.

425. Under existing subsection 105.4(5), to obtain a PDO to prevent a terrorist act, a terrorist act must be one that is 'imminent' (paragraph 105.4(5)(a)) and must be one that is 'expected to occur, in any event, at some time in the next 14 days' (paragraph 105.4(5)(b)). The threshold places an emphasis on a particular time a terrorist act is expected to occur.

426. The purpose of the amendments in this Schedule is to amend the requirements in subsection 105.4(5) by replacing subsection 105.4(5) and the 'imminent test' with a threshold that focusses on the capability of a person to commit a terrorist act as opposed to the specific time the terrorist act is expected to occur.

**Item 1 – Subsection 105.1(a)**

427. This is a consequential amendment. Item 1 replaces the reference to 'imminent terrorist act' in paragraph 105.1(a) with a reference to the redefined phrase 'terrorist act', which characterises the nature of the threats that warrant the imposition of a PDO. That is, the object of Division 105 is to allow a person to be taken into custody and detained for a short period of time in order to 'prevent a terrorist act that is capable of being carried out, and could occur, within the next 14 days from occurring'. This captures the meaning given to 'terrorist act' under subsection 105.4(5). The purpose and intended operation of the test in subsection 105.4(5) are detailed at item 2.

**Item 2 – Subsection 105.4(5)**

*Clarification of the nature of the terrorist act*

428. The ordinary meaning of 'imminent' is 'likely to occur at any moment'. It has two components. The first component is a preparedness component—the act needs to be capable of occurring or be at a certain stage of readiness. The second component is temporal—the act is likely to occur at any time. Paragraph 105.4(5)(b) puts an outer limit on the temporal aspect of 'imminent' so although it is likely to occur at any time, it is expected to occur within 14 days. The policy rationale for this threshold is to capture terrorist acts that are capable of occurring and that are also temporally close. This gives the PDO regime an inherently preventative character. However, the provisions are confusing as paragraphs 105.4(5)(a) and (b) both have temporal aspects. Given paragraph 105.4(5)(b) places an outer limit on the temporal component of imminent, the only work left for paragraph 105.4(5)(a) to do is to reflect that the act has to have reached a certain stage of readiness.

429. Current subsection 105.4(5)(b) can also be interpreted as imposing impractical constraints on law enforcement agencies. It requires an expectation that an event will occur

in the next 14 days. However, law enforcement agencies may be aware of individuals who intend to commit terrorist acts and who possess the necessary ability to carry out a terrorist act, but who have no clear timeframe in mind as to when they might perpetrate the act. The terrorist act could potentially occur within hours, weeks or months. For example, if a terrorist is prepared and waiting for a signal or instruction to carry out their act, the AFP may not be able to identify when that signal or instruction will be sent. Indeed the terrorist themselves may not know. In other circumstances, a person may become aware that they are the subject of law enforcement surveillance and accordingly change the timing of the planned attack to evade attention. In such instances, law enforcement agencies may not be able to obtain a PDO as the issuing authority may not be satisfied that there is an expectation the act will occur within precisely 14 days, despite the clear and ongoing threat posed by the individual.

430. The current focus of subsection 105.4(5) on the specific timing for when an act will occur within a certain period, rather than the capability for an act to occur within a certain period, is problematic. There is an operational gap in the ability to deal with terrorist acts that are not planned to occur on a particular date, even where the preparations for that terrorist act may be in the final stages or complete.

431. Item 2 replaces the 'imminent' test in subsection 105.4(5) with a requirement that the terrorist act is 'capable of being carried out, and could occur, within the next 14 days'. The amended test still captures the essence of the original imminent test by having both a preparedness component and a temporal component. The preparedness component is that the terrorist act is capable of being carried out. The temporal component is that it could occur within 14 days.

432. The version of this Bill that had previously been before Parliament originally retained the word 'imminent' to describe the required nature of the terrorist act in new subsection 105.4(5). Following Recommendation 15 of the Committee advisory report, the word 'imminent' was been removed. The Committee accepted the current limitations on the efficacy of the PDO regime occasioned by the existing 'imminent' test. It further supported the policy rationale in the new test in subsection 105.4(5) with its increased focus on the capability of a terrorist act to occur as opposed to merely its temporal features. However, so as to not stretch the meaning of the term 'imminent' beyond its ordinary usage, the Committee recommended that the test not use the term 'imminent' to describe the required nature of the terrorist act.

*Thresholds*

433. The current structure of 105.4 may also cause confusion about the relevant threshold for the requirement under existing subsection 105.4(5). Two separate interpretations are possible. The first is that the requirements under subsection 105.4(5) standalone from the rest of section 105.4 and must be established as a matter of fact.

434. Alternatively, subsection 105.4(5) may be interpreted such that the thresholds for the AFP member and issuing authority are to be read into the requirements in existing subsection 105.4(5). These thresholds are respectively, 'suspects, on reasonable grounds' for an AFP member (see existing paragraph 105.4(a)) and 'reasonable grounds to suspect' for an issuing authority (see existing paragraph 105.4(b)).

435. Item 2 clarifies the provisions by clearly articulating that the test in subsection 105.4(5) must be read in conjunction with the thresholds applicable to the AFP member and issuing authority. That is:

- the AFP member 'suspects, on reasonable grounds' that:
    - a terrorist act is capable of being carried out within the next 14 days, and
    - a terrorist act could occur within the next 14 days.
- the issuing authority has 'reasonable grounds to suspect' that:
    - a terrorist act is capable of being carried out within the next 14 days, and
    - a terrorist act could occur within the next 14 days.

436. The item also clarifies the interaction between subsection 105.4(5) and paragraph 105.4(4)(c) as follows:

- the AFP member must be satisfied that the making of the order would substantially assist in preventing a terrorist act (being a terrorist act that the AFP member 'suspects, on reasonable grounds' is capable of being carried out within the next 14 days and could occur within the next 14 days), and
- the issuing authority must be satisfied that the making of the order would substantially assist in preventing a terrorist act (being a terrorist act that the issuing authority has 'reasonable grounds to suspect' is capable of being carried out within the next 14 days and could occur with the next 14 days.

## Schedule 6—Issuing authorities for preventative detention orders

### *Criminal Code Act 1995*

### Overview

438. Under existing subsection 105.2(1), a serving or retired judge of the Family Court of Australia (Family Court) may be appointed as an issuing authority for continued PDOs. While other courts or persons listed in subsection 105.2(1) exercise functions relevant to the areas of criminal law and counter-terrorism, the Family Court does not typically exercise jurisdiction in relation to these matters. It is anomalous for a judge of the Family Court to play a role in the PDO regime, and no Family Court judge has ever been appointed under section 105.2.

439. These amendments remove this anomaly and ensure that only those judges who have served in a court which ordinarily exercises criminal jurisdiction will be eligible for appointment as an issuing authority for PDOs.

### Item 1 – Subsection 100.1(1) of the *Criminal Code* (definition of *Judge*)

440. This item repeals the definition of 'Judge' in subsection 100.1(1) of the *Criminal Code*. A definition is no longer required as explicit reference is given to which judges are eligible or permitted to perform various functions throughout Part 5.3 of the *Criminal Code*.

### Item 2 – Subsection 100.1(1) of the *Criminal Code* (paragraph (c) of the definition of *superior court*)

441. This item removes the Family Court of Australia or of a State from the definition of 'superior court' in paragraph 100.1(1)(c) of the *Criminal Code*. A 'superior court' will be defined as the High Court, the Federal Court, the Supreme Court of a State or Territory, or the District Court (or equivalent) of a State or Territory.

442. The purpose of this amendment is to remove the Family Court from the list of superior courts in which a person must have served as a judge before becoming eligible to be appointed as an issuing authority for continued PDOs under paragraph 105.2(1)(d). Currently, a person who has served as a judge of the Family Court for at least five years may be appointed as an issuing authority under section 105.2, with various powers including the power to make and extend a continued PDO. This amendment ensures retired judges of the Family Court are ineligible to be appointed as issuing authorities for continued PDOs.

### Item 3 – Paragraph 105.2(1)(b) of the *Criminal Code*

443. This item amends paragraph 105.1(1)(b) by replacing the words 'a person who is a Judge' with the words 'a person who is a Judge of the Federal Court of Australia or of the Federal Circuit Court of Australia'. This amendment, in conjunction with existing paragraph 105.1(1)(a), clarifies that only serving judges of a State or Territory Supreme Court, the Federal Court or Federal Circuit Court of Australia are eligible to be appointed as issuing authorities for continued PDOs.

**Schedule 7—Application of amendments of the *Criminal Code***

***Criminal Code Act 1995***

**Item 1 – At the end of Division 106 of Part 5.3 of the *Criminal Code***

444. This item inserts an application provision, 'Application provision for certain amendments in the Counter-Terrorism Legislation Amendment Act (No. 1) 2016', for the amendments to Division 104 of the *Criminal Code*.

445. New section 106.7 specifies how and when certain amendments to Divisions 104 and 105 will operate following commencement of those amendments.

446. New subsection 106.7(1) provides that the amendments to the control order regime made by Schedules 2 and 3 apply to an order made under Division 104 after the commencement of this section where the order is requested after commencement, and whether the conduct in relation to which that request is made occurs before or after commencement. Schedules 2 and 3 amend Division 104 to permit control orders to be imposed on persons younger than 16 years of age, and to impose certain obligations on a person required to wear a tracking device under a control order, respectively.

447. This means, for example, a request could be made to make an interim control order in relation to a young person 15 years of age after the commencement of this section based on information about the young person's conduct that occurred before commencement.

448. New subsection 106.7(2) clarifies that, despite the amendment made by Schedule 4, which removes the authority of a Family Court to issue control orders, Division 104 continues to apply, as if the amendment had not been made, in relation to any of the following:

- a request for an interim control order, where the request was made before the commencement of this section
- the making of an interim control order in response to such a request
- the making of a declaration in relation to such an interim control order
- the revocation of such an interim control order
- the confirmation of such an interim control order (with or without variation)
- the making of a confirmed control order that corresponds to such an interim control order that has been so confirmed
- the revocation or variation of such a confirmed control order, and
- any other proceedings under that Division that are associated with, or incidental to, a matter covered by any of the above paragraphs.

449. This ensures that any matter already on foot in relation to a control order that is before the Family Court can continue despite removal of the Family Court as an issuing authority.

450. New subsection 106.7(3) provides that the reporting requirements in section 104.29 of the *Criminal Code* as amended by Schedule 8 of the Bill apply in relation to any year that ends on 30 June after commencement of section 106.7.

451. New subsection 106.7(4) provides that Division 105 of the *Criminal Code*, as amended by Schedule 5, applies in relation to an application for a PDO, an initial PDO, an extension of an initial preventative detention, a continued PDO or an extension of a continued PDO after the commencement of section 106.7. The amendments to section 105.4 made by Schedule 5 clarify the threshold for applying for a PDO. This application provision ensures the new threshold can be relied upon for any application for a new, extended or continued preventative detention after the commencement of section 106.7.

**Schedule 8—Monitoring of compliance with control orders etc.**

***Crimes Act 1914***

**Overview**

452. Division 104 of Part 5.3 of the *Criminal Code* provides for the imposition of a range of obligations, prohibitions and restrictions on a person as part of a control order to protect the public from a terrorist act, prevent terrorism or prevent engagement in hostile activities overseas. The Crimes Act and other Commonwealth legislation confer a range of investigatory powers on law enforcement and other agencies, including the search warrant regime in Division 2 of Part IAA of the Crimes Act. However, Australian law does not provide adequate powers for law enforcement agencies to monitor compliance with controls under a control order to sufficiently reduce the risk that a person will engage in terrorist act planning or preparatory acts while subject to a control order.

453. The amendments in this Schedule create a 'monitoring warrant' regime in new Part IAAB of the Crimes Act to apply to individuals subject to a control order under Division 104 of Part 5.3 of the *Criminal Code*. Unlike the existing search warrant regime, the new regime will not require the issuing authority to be satisfied that an offence has already occurred or is going to be committed. Rather, this regime will be targeted at monitoring compliance with the conditions of a control order for the purposes of preventing a person from engaging in terrorist act planning or preparatory acts.

454. The regime is modelled on the monitoring regime in the RPSP Act and the existing search warrant provisions in the Crimes Act. The SD Act and the TIA Act are also being amended by this Bill to confer powers on law enforcement agencies to monitor compliance with control orders.

**Item 1 – Part IAAB—Monitoring of compliance with control orders etc.**

455. This item inserts a new 'Part IAAB—Monitoring of compliance with control orders etc.' after Part IAAA of the Crimes Act.

456. The proposed new 'monitoring' regime inserted in the Crimes Act will only apply to individuals subject to a control order. Unlike the existing search warrant regime in the Crimes Act, the new regime will not require the issuing authority to be satisfied that an offence has already occurred or is going to be committed. Rather, this regime will be targeted at monitoring compliance for the purposes of preventing a person from engaging in terrorist act planning or preparatory acts while subject to a control order.

457. Given the gravity of the purposes for which a control order is made, compliance with its terms is clearly important. If compliance could only be monitored once there are reasonable grounds upon which to suspect a breach, the damage would have been done and the protective value of the order would be undermined. The protective value of a control order is also enhanced by the subject of the control order knowing that compliance may be more readily monitored.

458. The regime is closely modelled on the existing provisions in the RPSP Act. That regime sets out a range of powers relevant to monitoring, investigation and enforcement purposes. The powers in relation to entry and inspection by consent or under a monitoring

warrant are modelled on the powers in the RPSP Act. The powers in relation to seizure for evidentiary purposes (which can only be exercised under a monitoring warrant—not where entry was by consent) are modelled on the existing search warrant regime in Part IAA of the Crimes Act.

**Part IAAB—Monitoring of compliance with control orders etc.**

**Division 1—Introduction**

459. Division 1 sets out a simplified outline and relevant definitions for the new Part IAAB. The Division provides the criteria for determining whether a person has a 'prescribed connection' with a premises, provides that a person's privileges against self-incrimination or legal professional privilege enshrined in common law are not abrogated by Part IAAB, and provides that Part IAAB is not intended to limit or exclude the operation of another law of the Commonwealth which confers similar powers to those conferred by Part IAAB.

**3ZZJA Simplified outline of this Part**

460. Section 3ZZJA provides an outline of the new Part IAAB of the Crimes Act which creates a framework of monitoring of compliance with control orders.

461. While simplified outlines are included to assist readers to understand the substantive provisions, the outlines are not intended to be comprehensive. It is intended that readers should rely on the substantive provisions.

**3ZZJB Definitions**

462. Section 3ZZJB contains a number of definitions relevant to the new provisions in Part IAAB.

463. The expressions, 'confirmed control order', 'control order' and 'interim control order' each have the same meaning as in Part 5.3 of the *Criminal Code*.

464. The expression 'damage', in relation to data, includes damage by erasure of data or addition of other data.

465. The phrase 'engage in a hostile activity' has the same meaning as in Part 5.3 of the *Criminal Code*, which cross-refers readers to the definition set out in subsection 117.1(1) of the *Criminal Code*, and the phrase 'foreign country', when used in the expression 'hostile activity in a foreign country', also has the same meaning as in the *Criminal Code*.

466. The expressions 'evidential material', 'frisk search', 'ordinary search', 'strip search' and 'seizable item' have the same meanings as in Part IAA.

467. The expression 'issuing officer' means a magistrate.

468. When used in relation to premises, the term 'monitoring powers' has the meaning given by sections 3ZZKB, 3ZZKC and 3ZZKD. When used in relation to a person, monitoring powers has the meaning given by section 3ZZLB.

469. A 'monitoring warrant' means a warrant under new section 3ZZOA or 3ZZOB.

470. The term ‘premises’ reflects the definition in the RPSP Act, and includes a structure, building or conveyance, a place (whether or not enclosed or built on), or a part of a structure, building, conveyance or place.

471. A ‘prescribed connection with premises’ has the meaning given by new section 3ZZJC.

472. The term ‘recently used conveyance’ specifies the timeframe a constable has to conduct a search of a conveyance, which a person under new section 3ZZLA had operated or occupied.

473. The term relevant data has the meaning given by new subsection 3ZZKC(3).

**3ZZJC Prescribed connection with premises**

474. Section 3ZZJC outlines the circumstances in which a person has a ‘prescribed connection’ with premises for the purposes of Part IAAB.

475. Normally a warrant simply identifies the premises. However, this provision ensures that there is a connection between the premises and the person subject to the control order, even if that connection may be only temporary, for example, where the person is merely staying with friends for a short period of time.

476. Before a warrant can be issued, one of the following prescribed connections must be demonstrated between the person the subject of the control order and the premises:

- the person is the legal or beneficial owner of the premises
- the person has a legal or equitable estate or interest in the premises
- the person occupies, or resides on, the premises
- the person has possession or control of the premises
- the person performs employment duties on the premises
- the person carries on a business on the premises
- the person performs voluntary work on the premises, or
- the premises are used by a school, college, university or other educational institution; and the person attends the premises in his or her capacity as a student at the school, college, university or other educational institution.

477. Establishing one of these connections is necessary to ensure law enforcement cannot obtain a monitoring warrant in relation to premises that do not have a real and relevant connection to a person the subject of a control order.

**3ZZJD Privileges not abrogated**

478. New section 3ZZJD confirms that certain common law privileges are preserved.

479. Subsection 3ZZJD(1) is based on subsection 17(1) of the RPSP Act. This subsection makes clear that the right to claim privilege against self-incrimination, as enshrined in common law, has not been abrogated under this Part. This means that a person

has the right to refuse to answer a question or provide information or documents if that answer, information or document might incriminate that person or make them liable to a penalty.

480. Subsection 3ZZJD(2) is based on subsection 17(2) of the RPSP Act. This subsection makes clear that the right to claim legal professional privilege, as provided by the common law, has not been abrogated under this Part. This means that a person has the right to refuse to answer a question, give information, or produce a document on the ground that the answer, information or document would be subject to legal professional privilege.

481. Subsection 3ZZJD(3) is based on subsection 17(3) of the RPSP Act. This subsection makes clear that the inclusion of subsections 3ZZJD(1) and (2) in Part IAAB does not imply that the privilege against self-incrimination or legal professional privilege is abrogated in any other law of the Commonwealth.

**3ZZJE Application of Part**

482. This section makes clear that Part IAAB should not limit or exclude the operation of another law of the Commonwealth (including other provisions of this Act) relating to the search of premises, the searching of persons or conveyances, the seizure of things, or the requesting of information or documents from persons.

**Division 2—Powers of constables in relation to premises**

483. This Division specifies the monitoring powers, and powers to ask questions and seek production of documents, conferred on constables who enter premises by consent or under a warrant.

**Subdivision A—Monitoring powers**

**3ZZKA Entering premises by consent or under a warrant**

484. Under this regime modelled on the RPSP Act, the AFP can enter premises and exercise a number of powers by consent.

485. New section 3ZZKA authorises constables to enter the premises and exercise monitoring powers for the protection of the public from a terrorist act, preventing the provision of support for or the facilitation of a terrorist act or the engagement in a hostile activity in a foreign country or to determine compliance with a control order.

486. The section specifies that a constable may only enter the premise if there is a control order in force in relation to a person, the person has a prescribed connection with particular premises and is authorised. Authorisation to enter the premises is provided if either the occupier of the premises consents to the entry, or the entry is authorised by a monitoring warrant.

487. The explanatory note to this section makes clear that an authorised person must leave the premises if entry to the premises was with the occupier's consent and that consent has been withdrawn (see section 3ZZNA).

### 3ZZKB General monitoring powers

488. Section 3ZZKB sets out the monitoring powers that a constable can exercise in relation to premises entered by consent or under a warrant.

489. The monitoring powers are modelled on the general monitoring powers listed in section 19 of the RPSP Act and permit a constable to, among other things, search premises, bring equipment and materials on to the premises, measure or test any 'thing' on the premises, photograph things or make copies of documents, or operate electronic equipment.

490. Section 3ZZKB provides a police constable with two additional powers, specifically the power to search for and record fingerprints found at the premises and the power to take samples of things found at the premises, which are akin to powers provided by existing paragraph 3F(1)(b) of the Crimes Act. Samples may include such things as samples of explosive and weapon-type material, and DNA from such items as used cups or cigarettes. These additional powers are appropriate for terrorism related offences due to the extraordinary risk posed to the Australian community by acts of terrorism, and are considered critical to the success of certain investigations by the AFP.

491. Pursuant to section 3ZZKG, a person who is not a constable and is assisting a constable in the execution of a monitoring warrant can exercise the powers listed in section 3ZZKB.

### 3ZZKC Operating electronic equipment

492. Section 3ZZKC authorises a constable to operate electronic equipment on the premises and to use a disk, tape or other storage device that is on the premises and can be used with the equipment or is associated with it. In this context, electronic equipment primarily refers to, but is not limited to, data storage equipment such as computers that may have information relevant to monitoring compliance. This power is necessary to ensure a constable can obtain access to electronic records that are relevant to the protection of the public from a terrorist act, preventing the provision of support for or the facilitation of a terrorist act or the engagement in a hostile activity in a foreign country or to determine compliance with a control order.

493. A constable's power to operate electronic equipment extends to copying data from the electronic equipment onto storage devices. However, a constable may only operate electronic equipment if he or she reasonably believes this can occur without damaging the equipment.

494. The explanatory note to this section makes clear that the owner of the equipment may receive compensation for damage in accordance with section 3ZZNF.

### 3ZZKD Securing electronic equipment to obtain expert assistance

495. Section 3ZZKD mirrors section 21 of the RPSP Act. Section 3ZZKD applies where a constable enters premises under a monitoring warrant.

496. Subsection 3ZZKD(1) provides that a constable may secure electronic equipment on the premises provided the criteria set out in the subsection are met, including that expert assistance is required to operate the equipment.

497. Subsection 3ZZKD(3) requires the constable to give notice to the occupier or a person who represents the occupier of the intention to secure the equipment for up to 24 hours.

498. Subsection 3ZZKD(4) provides that the equipment can only be secured until the expert can operate the equipment or the 24-hour period has elapsed, whichever occurs first.

499. Subsection 3ZZKD(5) enables a constable to apply to an issuing officer for an extension of the 24-hour period if the constable believes on reasonable grounds that the equipment needs to be secured for longer than that period. An extension may be sought and granted more than once (subsection 3ZZKD(7)).

500. Subsection 3ZZKD(6) requires the constable to notify the occupier of the premises, or their apparent representative, of their intention to apply for an extension. This provides a means by which an occupier can challenge an application for extension if they so choose.

**Subdivision B—Powers to ask questions and seek production of documents**

**3ZZKE Asking questions and seeking production of documents**

501. Section 3ZZKE authorises a constable to ask questions and seek documents where the constable enters premises either by consent or under a monitoring warrant (under section 3ZZKA).

502. If a constable enters premises with the consent of the occupier, subsection 3ZZKE(2) provides that a constable may ask the occupier to answer any questions or produce documents that are likely to assist in the protection of the public from a terrorist act, preventing the provision of support for or the facilitation of a terrorist act or the engagement in a hostile activity in a foreign country or to determine compliance with a control order. There is no requirement for the person to answer the question or produce the document where entry was undertaken by consent. Accordingly, the other subsections within this section do not apply to subsection 3ZZKE(2).

503. The first note to subsection 3ZZKE(2) advises readers that a person is not required to answer a question or produce a document under this subsection. The second note refers readers to sections 3ZZRC and 3ZZRD, which deal with using, sharing and returning documents produced under Part IAAB and answers to questions asked under section 3ZZKE, respectively.

504. If entry is authorised by a monitoring warrant, subsection 3ZZKE(3) provides that a constable may require any person on the premises to answer any questions or produce documents that are likely to assist in the protection of the public from a terrorist act, preventing the provision of support for or the facilitation of a terrorist act or the engagement in a hostile activity in a foreign country or to determine compliance with a control order. Subsection 3ZZKE(3) is subject to subsections (4) and (7).

505. The note refers readers to sections 3ZZRC and 3ZZRD, which deal with using, sharing and returning documents produced under Part IAAB and answers to questions asked under section 3ZZKE, respectively.

506. Subsection 3ZZKE(4) qualifies that before a constable requires a person to answer a question or produce a document under subsection (3), the constable must explain to the

person the effect of section 3ZZJD concerning self-incrimination and legal professional privilege.

507. Subsection 3ZZKE(5) provides a safeguard to the person by stipulating that if a constable fails to explain the effect of section 3ZZJD then any answer to a question or document produced under this section is not admissible in evidence against the person in criminal proceedings.

508. The note again refers readers to sections 3ZZRC and 3ZZRD, which deal with using, sharing and returning documents produced under Part IAAB and answers to questions asked under section 3ZZKE, respectively.

509. Subsection 3ZZKE(6) qualifies the requirement to answer questions and produce documents by providing that a person is not required to answer or produce a document if the person does not possess the information or document required and has taken reasonable steps to obtain the required information or documents without success. Subsection 3ZZKE(7) further qualifies the requirement by providing that a person is not required to produce a document if the document sought is not at the premises.

510. Subsection 3ZZKE(8) provides that a person commits an offence for failing to comply with a requirement under subsection 3ZZKE(3). This offence carries a penalty of 30 penalty units. The note to this offence notes that this section does not abrogate the privilege against self-incrimination or legal professional privilege (as per section 3ZZJD).

511. This section is limited to constables. The powers in this section do not extend to persons who are not constables but are assisting a constable in the execution of a monitoring warrant.

**Subdivision C—Other powers**

**3ZZKF Other powers**

512. This section authorises constables to exercise additional powers modelled on the standard search warrant regime in Part IAA of the Crimes Act.

513. The effect of subsection 3ZZKF(1) is that, while the powers are available whether the initial entry was by consent or under a monitoring warrant, these powers can only be exercised where a monitoring warrant is in force.

514. Subsection 3ZZKF(2) authorises a constable to seize items where they suspect on reasonable grounds to be evidential material (including evidential material within the meaning of the *Proceeds of Crime Act 2002* (POCA)), tainted property within the meaning of the POCA, and seizable items, found during the exercise of the monitoring powers on the premises.

515. Subsection 3ZZKF(2) also authorises the constable to conduct an ordinary or frisk search of a person at or near the premises if the constable suspects on reasonable grounds that the person has any evidential material or seizable items in his or her possession, in circumstances when a constable enters premises under section 3ZZKA and the entry is authorised by a monitoring warrant. A seizable item is defined in Part IAA of the Crimes Act as anything that would present a danger to a person or that could be used to assist a person to escape from lawful custody. A constable can seize things found during that search or frisk

search of a person if the constable suspects on reasonable grounds that the thing is evidential material (including evidential material within the meaning of the POCA), tainted property within the meaning of the POCA or seizable items.

516. Reference to powers under subsection 3ZZKF(2) in relation to premises includes the powers referred to in paragraphs (2)(b) and (c), even if those powers are not exercised on the premises.

517. These powers can only be exercised by a constable, and not a person assisting.

**3ZZKG Availability of assistance and use of force in executing a warrant**

518. This section, which is based on existing sections 3G and 3ZZCD of the Crimes Act, authorises a constable to obtain such assistance as is necessary and reasonable in the circumstances to execute the warrant. It also authorises a constable to use such force against people and things as is necessary and reasonable to execute a monitoring warrant or other powers set out in section 3ZZKF. For example, a constable may need assistance in lifting or opening something during the execution of the warrant.

519. The effect of subsection 3ZZKG(1) is that, while assistance is available whether the initial entry was by consent or under a monitoring warrant, it can only be obtained where a monitoring warrant is in force.

520. Subsection 3ZZKG(2) authorises constables to use reasonable and necessary force against both persons and things. This would allow, for example, a constable to use force that is reasonable and necessary in the circumstances to restrain a violent person during the execution of the warrant.

521. Subsection 3ZZKG(3) limits the circumstances where assistance can be obtained to circumstances where it is necessary and reasonable in the circumstances.

522. Subsection 3ZZKG(4) sets out what a person who is not a constable and who has been authorised to assist in the execution of the warrant, can do. Such a person can enter the relevant premises (paragraph 3ZZKG(4)(a)), exercise monitoring powers (paragraph 3ZZKG(4)(b)), and use force against things (paragraph 3ZZKG(4)(c)). For example, a person who is not a constable may need to use force to access a locked filing cabinet in order to inspect the documents inside.

523. Paragraph 3ZZKG(5)(a) authorises a person assisting who is not a constable to secure electronic equipment pursuant to subsection 3ZZKD(2) if the constable forms the suspicion mentioned in that subsection.

524. Paragraph 3ZZKG(5)(b) excludes a person who is not a constable from applying for an extension of the period in which equipment may be secured pursuant to subsection 3ZZKD(5). Section 3ZZOA authorises a constable to apply to an issuing officer for a monitoring warrant which allows electronic equipment to be secured. It would be inconsistent with that provision to allow a person other than a constable to apply for an extension of the period in which electronic equipment may be secured pursuant to the monitoring warrant. Paragraph 3ZZKG(5)(b) provides that an authorised person who is not a constable must not exercise the power to ask the occupier of the premises questions or request they produce documents pursuant to section 3ZZKE, or seize evidential material,

things believed on reasonable grounds to be evidential material or tainted property pursuant to section 3ZZKF. For example, it would be inappropriate for a person other than a constable to question a person, in circumstances where a person's response might be of evidentiary value.

525. Subsection 3ZZKG(6) provides that any action validly taken by a person assisting the constable in respect of this power is taken to be done by the constable.

**Division 3—Powers of constables in relation to persons subject to control orders**

**3ZZLA Searching a person by consent or under a warrant**

526. Under this section a constable can conduct an ordinary search or a frisk search of a person who is subject to a control order and exercise the monitoring powers outlined in section 3ZZLB if the person consents or a monitoring warrant is in place. A search can only be undertaken for one of the listed purposes, which are protecting the public from a terrorist act, preventing support or facilitation of a terrorist act or the engagement in a hostile activity in a foreign country, or determining compliance with the control order.

527. Only a constable can physically search a person and if practicable the search must be conducted by a person of the same sex (see section 3ZZTA).

**3ZZLB Monitoring powers**

528. Section 3ZZLB sets out the monitoring powers exercisable by a constable when conducting an ordinary search or a frisk search in accordance with section 3ZZLA. This section authorises a constable to search things in the person's possession, search a recently used conveyance, record fingerprints and take samples from things.

**3ZZLC Seizure powers**

529. This section authorises a constable to seize certain things located during the search of a person or a recently used conveyance under section 3ZZLA.

530. Section 3ZZLC authorises a constable to seize evidential material or seizable items, found in the course of the search, and other things found on or in the possession of the person or the recently used conveyance including evidential material or tainted property within the meaning of the POCA. A seizable item is defined in Part IAA of the Crimes Act as anything that would present a danger to a person or that could be used to assist a person to escape from lawful custody.

**3ZZLD Availability of assistance and use of force in executing a warrant**

531. This section authorises the use of assistance, including from a person who is not a constable, in searching persons and recently used conveyances under monitoring warrants.

532. Subsection 3ZZLD(2) provides that, when executing a warrant and exercising the seizure powers under section 3ZZLC, a constable can use reasonable and necessary force against persons and things. In addition, the constable can obtain assistance, including from persons who are not constables, in exercising those powers (subsection 3ZZLD(3)). However, a person who is not a constable can only exercise force against things (subsection 3ZZLD(4)). As the execution of a search of a person necessarily involves 'force'

against that person, this means a person who is not a constable cannot undertake a search of a person. In addition, a person who is not a constable is not authorised to seize items (subsection 3ZZLD(5)).

533. Any action validly taken in respect of this power is taken to have been done by the constable (subsection 3ZZLD(6)).

**Division 4—Obligations and incidental powers of constables**

534. Division 4 protects against arbitrary abuses of power as the entry, monitoring, search, seizure and information gathering powers provided in the new Part IAAB are conditional upon consent being given by the occupier of the premises or prior authorisation by a magistrate.

**3ZZNA Consent of occupier of premises**

535. Section 3ZZNA provides for entry based on the consent of the occupier.

536. Subsection 3ZZNA(1) provides that, before obtaining consent to enter premises, the constable must advise the occupier of his or her right to refuse consent.
Subsection 3ZZNA(2) reinforces this provision by providing that consent does not have effect unless it is voluntary.

537. The occupier of the premises can restrict entry by a constable to a particular period and the entry only has effect for that period unless it is withdrawn earlier (subsection 3ZZNA(3)). Where consent is not expressed to be limited in duration, it ceases when the occupier withdraws it (subsection 3ZZNA(4)). Any constables and other persons assisting must leave the premises if consent ceases to have effect (subsection 3ZZNA(5)).

538. Subsection 3ZZNA(6) specifically provides that if a constable does not show the occupier his or her identity card before entering the premises then they must do so as soon as reasonably practicable after entering the premises (this reflects standard practice).

**3ZZNB Consent to search of a person**

539. An ordinary search or a frisk search of a person may be exercised with the consent of the person pursuant to paragraph 3ZZLA(2)(a). Section 3ZZNB sets out the parameters for valid consent.

540. Subsection 3ZZNB(1) provides that, before obtaining consent to search a person, the constable must advise the occupier of his or her right to refuse consent.
Subsection 3ZZNB(2) reinforces this provision by providing that consent does not have effect unless it is voluntary.

541. Where a person restricts the constable's authority to search his or her person to a particular period, the consent only has effect for that period unless it is withdrawn earlier (subsection 3ZZNB(3)). Where consent is not expressed to be limited in duration, it ceases when withdrawn by the occupier (subsection 3ZZNB(4)).

**3ZZNC Announcement before entry under warrant**

542. Section 3ZZNC sets out the criteria for entering premises under a monitoring warrant.

543. The constable must announce that he or she has authority to search the premises (paragraph 3ZZNC(a)), show his or her identity card (paragraph 3ZZNC(b)), and give any person at the premises the opportunity to allow entry.

**3ZZND Constable to be in possession of warrant**

544. This section requires a constable to be in possession of the monitoring warrant or a copy of the warrant whilst executing the warrant.

**3ZZNE Details of warrant etc. to be given to occupier**

545. Section 3ZZNE requires a constable executing a monitoring warrant to provide a copy of the warrant as soon as practicable to the occupier of the premises, or an occupier's apparent representative, if either is present.

**3ZZNF Compensation for damage to electronic equipment**

546. Section 3ZZNF provides that a person is entitled to compensation for damage to electronic equipment, or data recorded on the equipment and compensation for damage or corruption of programs associated with the use of the equipment or data.

547. Subsections 3ZZNF(2) to (4) make it clear that compensation is limited to circumstances where the damage or corruption to the equipment, data or programs occurred because insufficient care was exercised in either selecting the person to operate the equipment or in the operation of the equipment. This recognises the fact that powers to operate electronic equipment do not excuse damage caused by a lack of care. Subsection 3ZZNF(3) acknowledges that, if the Commonwealth and the owner of the equipment or user of the data do not agree on reasonable compensation which the Commonwealth must pay, the owner may institute proceedings in the Federal Court of Australia, the Federal Circuit Court of Australia or a court of a State or Territory that has jurisdiction in relation to the matter. Subsection 3ZZNF(4) sets out matters relevant to the quantum of compensation payable.

**3ZZNG Occupier entitled to be present during search**

548. This section provides the right for the occupier of the premises or their apparent representative, who is present when a warrant is executed, to observe the execution of the warrant on the premises. This right does not limit how the warrant may be executed or require an occupier to witness all of a constable's activities, but it does recognise that a person should not be excluded during the execution of a warrant unless they attempt to obstruct the inspection.

549. For the purposes of this section 'an occupier' or another person who apparently represents the occupier, can be someone other than the person who is subject to the control order. For example, if the person the subject of the control order lives in a house with other individuals, those individuals are entitled under this section to be present during the search of the premises.

**3ZZNH Person subject to a control order is entitled to be present during search**

550. This section provides that, where a search of premises is undertaken under a monitoring warrant, the person the subject of the relevant control order is entitled to be present.

**Division 5—Monitoring warrants**

**3ZZOA Monitoring warrant in relation to premises**

551. This section allows for a constable to apply to an issuing officer for a warrant which will allow monitoring of the control order to prevent breaches and, consequently, to prevent things such as the facilitation of a terrorist act or the engagement in hostile activity in a foreign country.

552. Subsection 3ZZOA(2) provides that in order to issue the warrant the issuing officer must be satisfied that a control order is in force, the person has a prescribed connection with the premises and having regard to a number of matters, it is reasonably necessary that one or more constables have access to the premises for a particular purpose.

553. The matters the issuing officer must have regard to are the nature of the person's connection with the premises, one or more of the matters set out in paragraphs 3ZZOA(4)(a)-(f), the matter set out in new paragraph 3ZZOA(4)(g), and any other matters the issuing officer considers relevant. The matters set out in paragraphs 3ZZOA(4)(a)-(f) include the possibility that the person has, is, or will engage in, provide support for, or facilitate, a terrorist act or engagement in a hostile activity overseas. Paragraph 3ZZOA(4)(g) relates to whether allowing one or more constables to have access to the premises, and exercise the monitoring powers in relation to the premises, would be likely to have the least interference with any person's liberty and privacy that is necessary in the circumstances.

554. The positive requirement to consider whether execution of a monitoring warrant constitutes the least interference with the liberty or privacy of a person that is necessary in the circumstances implements Recommendation 9 of the Committee advisory report.

555. The term 'least interference' is to be given its ordinary meaning.

556. The issuing officer must consider it reasonably necessary for one or more constables to have access to the premises for a purpose including the protection of the public from a terrorist act, or preventing the provision of support for, or the facilitation of, a terrorist act.

557. Subsection 3ZZOA(3) provides that the issuing authority may require further information concerning the grounds on which the issue of the warrant is being sought and must not issue the warrant until that information has been provided orally or by affidavit.

558. Subsection 3ZZOA(5) lists the matters that must be set out in the warrant, including a description of the premises to which the warrant relates, the time at which the warrant expires, whether a person who is not a constable is able to assist in executing the warrant, and details relating to the relevant control order.

559. Subsection 3ZZOA(6) provides a safeguard to ensure that information likely to prejudice national security is not required to be included in the warrant.
Subsection 3ZZOA(7) expressly provides that the warrant must state the date of expiry which

is no later than the end of the seventh day after the day on which it was issued. Subsection 3ZZOA(8) makes clear that successive warrants can be issued for the same premises.

**3ZZOB Monitoring warrant in relation to a person**

560. This section mirrors section 3ZZOA which allows a constable to apply to an issuing officer for a warrant which will allow monitoring of the control order to prevent breaches and, consequently, to prevent things such as the facilitation of a terrorist act or the engagement in hostile activity in a foreign country. However, section 3ZZOB relates to the issuance of a warrant in relation to a person.

561. Section 3ZZOB provides that in order to issue the warrant the issuing officer must be satisfied that a control order is in force and having regard to a number of matters, it is reasonably necessary that a constable should conduct an ordinary search or a frisk search of the person.

562. The matters the issuing officer must have regard to are one or more of the matters set out in paragraphs 3ZZOB(4)(a)-(f), the matter set out in new paragraph 3ZZOB(4)(g), and any other matters the issuing officer considers relevant. The matters set out in paragraphs 3ZZOB(4)(a)-(f) include the possibility that the person has, is, or will engage in, provide support for, or facilitate, a terrorist act or engagement in a hostile activity overseas. Paragraph 3ZZOB(4)(g) relates to whether allowing one or more constables to conduct an ordinary search or a frisk search of the person, and exercise the monitoring powers in relation to the person or a recently used conveyance, would be likely to have the least interference with any person's liberty and privacy that is necessary in the circumstances.

563. The positive requirement to consider whether execution of a monitoring warrant constitutes the least interference with the liberty or privacy of a person that is necessary in the circumstances implements Recommendation 9 of the Committee advisory report.

564. The term 'least interference' is to be given its ordinary meaning.

565. The issuing officer must consider it reasonably necessary for a constable to conduct a search of the person for a purpose including protecting the public from a terrorist act, preventing support or the facilitation of a terrorist act or a hostile activity in a foreign country, or determining whether the control order is being complied with.

566. Subsection 3ZZOB(3) provides that the issuing authority may require further information concerning the grounds on which the issue of the warrant is being sought and must not issue the warrant until that information has been provided orally or by affidavit.

567. Subsection 3ZZOB(5) lists the contents of the warrant, such as, the name of the person, the purpose for which the warrant is issued, the time at which the warrant expires, whether a person who is not a constable is able to assist in executing the warrant and details which relate to the control order.

568. Subsection 3ZZOB(6) provides a safeguard to ensure that information which is likely to prejudice national security is not stated in the warrant which will be disclosed. Subsection 3ZZOB(7) expressly provides that the warrant must state the date of expiry which is no later than the end of the seventh day after the day on which it was issued.

Subsection 3ZZOB(8) makes clear that successive warrants can be issued for the same person.

**3ZZOC Restrictions on personal searches**

569. This section expressly excludes a strip search or search of a person's body cavities pursuant to a monitoring warrant.

**3ZZOD Monitoring warrant must not be executed if the relevant control order is revoked etc.**

570. This section provides an important safeguard where the control order in relation to which a monitoring warrant was issued has since been revoked, declared void or varied by removing one or more of the obligations, prohibitions or restrictions.

571. Where a control order ceases to have effect, the grounds for the monitoring warrant will no longer exist. Similarly, if one or more of the obligations, prohibitions or restrictions imposed by the control order ceases to have effect, the grounds upon which the monitoring warrant was issued may no longer exist. Accordingly, it is appropriate that, in such circumstances, the legislation preclude the execution of the warrant. Where the control order is varied by removing one or more of the obligations, prohibitions or restrictions, it is open to the AFP to apply for a new monitoring warrant on the basis of the revised control order. This ensures the issuing authority has full visibility of the conditions imposed by the control order and whether it is appropriate to issue a warrant.

572. The provision does not extend to circumstances where a control order is varied by adding one or more additional obligations, prohibitions or restrictions. This is because the obligations, prohibitions and restrictions that were in force at the time the monitoring warrant was issued will continue in force, and it is reasonable and appropriate for the AFP to execute that warrant.

573. Subsections 3ZZOD(2), (3) and (4) provide that a thing seized, or information or document obtained, in breach of subsection 3ZZOD(1) is not admissible in evidence in a criminal proceeding other than a proceeding under subparagraph 3ZQU(1)(j) in relation to a complaint, allegation, or issue concerning using and sharing things seized and documents produced under Part IAA.

**Division 6—Monitoring warrants by telephone or other electronic means**

**3ZZPA Monitoring warrants by telephone or other electronic means**

574. The section authorises a constable to apply for a monitoring warrant by telephone, telex, fax or other electronic means of communication in cases of urgency or if the delay in making the application in person would frustrate the effective execution of the warrant. This inclusive description is designed to ensure other forms of electronic communication, including those not contemplated or not invented at the time of the amendment can be used to make an oral application.

575. This amendment clarifies that, under normal circumstances, an application should be made in writing in the presence of an issuing authority. However, where the situation is urgent, for example, because the person is thought to be about to abscond, destroy evidence or undertake actions in furtherance of a terrorist act, or because it is not possible to make an

application to an issuing authority in person within a reasonable period of time due to physical location or other limitations, an urgent oral application can be made.

576. Section 3ZZPA sets out the procedures by which a monitoring warrant may be obtained from an issuing officer by means of electronic communication, and a number of controls to ensure this form of warrant is valid and not misused.

577. Subsections 3ZZPA(3) and (4) reflect the existing provisions of subsections 3R(3) and (4) of the Crimes Act. The application must include all the information required in an ordinary application for monitoring warrant, but may be made before the information is sworn.

578. Pursuant to subsection 3ZZPA(5), after completing and signing the warrant, the issuing officer must inform the applicant by telephone, telex, fax or other electronic means, of the terms of the warrant and the day on which, and the time at which, the warrant was signed. The applicant must then complete a form of the monitoring warrant to reflect the warrant completed and signed by the issuing officer. As required in subsection 3ZZPA(6) this form must specify the name of the issuing officer who issued the warrant and the day and time of signing the warrant.

579. Subsection 3ZZPA(7) requires this completed form to be sent to the issuing officer, in addition to the information referred to when applying for the monitoring warrant which must have been duly sworn. These are to be sent by the end of the day after the day on which the warrant expires or the day after the day of execution of the warrant, whichever occurs first. Pursuant to subsection 3ZZPA(8), once received by the issuing officer, these documents must be attached to the form of warrant completed by the issuing officer. These provisions ensure appropriate accountability around monitoring warrants issued remotely.

**3ZZPB Offences relating to telephone warrants**

580. This section creates a range of offences relating to the form of monitoring warrants remotely authorised under section 3ZZPA. This includes detailing information that departs from the warrant authorised by the issuing officer. This offence has a maximum penalty of imprisonment for two years.

581. The creation of these offences safeguard against the inappropriate use of provisions relating to remote applications for monitoring warrants and ensures that the availability of these warrants required for operational urgency is balanced with the necessity of ensuring accountability for those officers applying for such warrants.

**Division 7—Extension of periods in which things secured**

**3ZZQA Extension of periods in which things secured**

582. This section provides for an issuing officer to grant an extension to the 24-hour period in which a thing can be secured by a constable. The issuing officer may require further information from the constable or some other person which demonstrates that the extension is necessary to prevent evidential material being destroyed, altered or interfered with.

583. Subsection 3ZZQA(4) outlines what must be included in an order for extending the period in which a thing is secured. This includes a description of the thing to which the order relates and the period for which the extension is granted.

**Division 8—Things seized, documents produced, and answers given, under this Part**

**3ZZRA Receipts for things seized under this Part**

584. To ensure a record of seizure is maintained and available to the person from whom material is seized, section 3ZZRA requires the constable to give a receipt for a thing that is seized when exercising powers under a monitoring warrant issued under new Part IAAB.

**3ZZRB Using, sharing and returning things seized under this Part**

585. This section provides that Division 4C of Part IAA of the Crimes Act applies to a thing seized under new Part IAAB. Division 4C of Part IAA specifies the purposes for which things and documents may be used and shared by a constable or Commonwealth officer, the requirements for operating seized electronic equipment, compensation for damaged electronic equipment, and the requirements for returning things seized or documents produced.

**3ZZRC Using, sharing and returning documents produced under this Part**

586. Similarly to section 3ZZRB, subsection 3ZZRC(1) provides that Division 4C of Part IAA of the Crimes Act applies to documents produced under new Part IAAB.

587. Subsection 3ZZRC(2) sets out the additional uses to which documents produced under section 3ZZKE can be put. Paragraphs 3ZZRC(2)(a) to (d) provide that a document produced under that section can also be used for the purposes of protecting the public from a terrorist act, preventing the provision of support for or the facilitation of a terrorist act or the engagement in a hostile activity in a foreign country, or to determine compliance with a control order. In addition, paragraph 3ZZRC(2)(e) authorises the document to be used for the purposes of preventing, investigating or prosecuting an offence

**3ZZRD Answers to questions asked under section 3ZZKE**

588. This section sets out the uses to which information provided in response to a question asked under either subsection 3ZZKE(2) or (3) can be put. Paragraphs 3ZZRD(a) to (d) provide that an answer to a question asked under those subsections can only be used for the purposes of protecting the public from a terrorist act, preventing the provision of support for or the facilitation of a terrorist act or the engagement in a hostile activity in a foreign country, or to determine compliance with a control order. In addition, paragraph 3ZZRD(e) authorises the answer to such a question to be used for the purposes of preventing, investigating or prosecuting an offence.

**Division 9—Powers of issuing officers**

**3ZZSA Powers of issuing officers**

589. This section is modelled on section 4AAA of the Crimes Act. Subsection 3ZZSA(1) provides that any function or power conferred on a magistrate under this Part is conferred in a personal capacity, that is, in *persona designata*, rather than as a court or a member of a court.

590. Subsection 3ZZSA(2) provides that the issuing officer does not need to accept the power conferred.

591. Subsection 3ZZSA(3) provides that a magistrate will have the same protection and immunity in relation to the performance or exercise of a function or power conferred on them under this Part as a magistrate would have if that function was exercised as a member of a court of which he or she was a member.

**Division 10—General**

**3ZZTA Conduct of ordinary searches and frisk searches**

592. This section provides that, if practicable, an ordinary or frisk search of a person pursuant to this Part must be conducted by a person of the same sex.

**3ZZTB Protection of persons—control order declared to be void**

593. This section provides a safeguard to protect the good faith actions or omissions of persons in the purported execution of a monitoring warrant or purported exercise of a consequential power, function or duty, where a court declares the interim control order on which the warrant was issued, to be void.

**3ZZTC Dealing with things, information or documents obtained under a monitoring warrant—control order declared to be void**

594. This section specifies certain purposes for which things seized, information obtained or a document produced pursuant to a monitoring warrant can be communicated or adduced as evidence where the court subsequently declares the interim control order void.

595. Subsection 3ZZTC(2) provides that where the conditions in subsection 3ZZTC(1) have been satisfied a person may adduce the thing, information or document as evidence in a proceeding or use or communicate the information or the contents of a document if the person reasonably believes that it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm (as defined in the *Criminal Code*) to a person or serious damage to property or for one or more purposes set out in subsection 3ZZTC (3).

596. Subsection 3ZZTC(3) outlines a number of other circumstances where a person may deal with the thing, information or document as necessary by adducing it as evidence, or using or communicating it. This subsection provides that dealing with the thing, information or document must be for the performance of a function or duty, or the exercise of a power, by a person, court, tribunal or other body under, or in relation to a matter arising under various pieces of Commonwealth and state and territory legislation, where the function, duty or power relates to a PDO.

**3ZZTD Commissioner to keep documents connected with issue of monitoring warrants**

597. This section provides that the AFP Commissioner must cause information about each monitoring warrant which is issued, revoked by instrument or extended, to be kept in AFP records. These record keeping requirements are consistent with existing record keeping requirements under the TIA Act and SD Act.

598. The record keeping requirements are intended to support the Commonwealth Ombudsman's oversight role and his or her ability to report to the Minister on the AFP's compliance with the requirements of the regime, as required under new section 3ZZUH.

599. This amendment implements part of Recommendation 11 of the Committee advisory report.

**3ZZTE Commissioner to notify Ombudsman in relation to monitoring warrants**

600. Subsection 3ZZTE(1) requires that within six months of a monitoring warrant being issued, the AFP Commissioner must notify the Commonwealth Ombudsman that the warrant has been issued and give the Ombudsman a copy of the warrant.

601. Subsection 3ZZTE(2) requires that as soon as practicable after an AFP member has contravened a provision of this Part, the AFP Commissioner must notify the Ombudsman of the contravention. A suspected contravention reported to or by the Ombudsman does not, *ipso facto*, give rise to, or imply legal liability.

602. Subsection 3ZZTE(3) provides that the AFP Commissioner's failure to comply with subsections 3ZZTE(1) and (2) does not affect the validity of a monitoring warrant.

603. The requirements at subsections 3ZZTE(1) and (2) support the Commonwealth Ombudsman's oversight role and his or her ability to report to the Minister on the AFP's compliance with the requirements of the regime, as required under new section 3ZZUH.

604. This amendment implements part of Recommendation 11 of the Committee advisory report.

**Division 11—Inspections by Ombudsman**

605. Division 11 provides the Commonwealth Ombudsman with inspection powers to support the Ombudsman's oversight role and sets out the requirements for the Ombudsman's annual report on the results of any inspections.

**3ZZUA Appointment of inspecting officers**

606. Section 3ZZUA allows the Ombudsman to appoint members of the Ombudsman's staff to be inspecting officers for the purpose of this Division. The appointment must be evidenced in writing.

**3ZZUB Inspection of records by the Ombudsman**

607. Section 3ZZUB establishes an inspection regime allowing the Commonwealth Ombudsman to inspect the records kept by the AFP to determine the extent of compliance by the AFP and members and special members of the Australian Federal Police with the provisions of new Part IAAB or any monitoring warrants. The role of the Ombudsman is to determine whether the records kept are accurate and whether the AFP is complying with its obligations under Part IAAB.

608. Paragraphs 3ZZUB(2)(a) and (b) provide that the Ombudsman can enter premises occupied by the AFP at any reasonable time after notifying the AFP Commissioner. The Ombudsman is then entitled to full and free access at all reasonable times to all records of the delayed notification search warrants scheme that are relevant to the inspection. The Ombudsman has the power under paragraph 3ZZUB(2)(c) to require a member of staff of the AFP to provide any information relevant to the inspection that is in their possession or to which the staff member has access.

609. Subsection 3ZZUB(3) requires the Commissioner to ensure that agency staff provide the Ombudsman with any assistance that the Ombudsman reasonably requires to enable the Ombudsman to inspect the records.

**3ZZUC Power to obtain relevant information**

610. Section 3ZZUC empowers the Ombudsman to require, in writing, a staff member of the AFP to provide written information relevant to an inspection at a specified place and within a specified period if the Ombudsman has reason to believe that the staff member is able to give the information.

611. Under subsections 3ZZUC(3) and 3ZZUC(5) the Ombudsman may also require, in writing, a staff member to attend to answer questions relevant to the inspection before a specified inspecting officer at a specified place and within either a specified period or at a reasonable time and date. This will enable the Ombudsman to question a staff member who he or she believes is able to give information relevant to the inspection.

612. If the Ombudsman has reasonable grounds to believe that a staff member, whose identity is unknown to the Ombudsman, is able to give information relevant to an inspection, subsections 3ZZUC(4) and 3ZZUC(5) also authorise the Ombudsman in writing to require the AFP Commissioner, or a person nominated by the AFP Commissioner, to attend to answer questions relevant to the inspection before a specified inspecting officer, at a specified place and either within a reasonable specified period or at a reasonable time and date.

**3ZZUD Offence**

613. Section 3ZZUD creates an offence if a person refuses or fails to attend before a person, to give information or to answer questions when required to do so under section 3ZZUC. The maximum penalty for the offence is imprisonment for six months.

**3ZZUE Ombudsman to be given information etc. despite other laws**

614. Subsection 3ZZUE(1) states that a person is not excused from providing information, answering questions or giving access to a document when required under this Division, on the grounds that doing so would contravene a law, would be contrary to the public interest or might tend to incriminate the person or make them liable to a penalty, or to disclose certain advice of a legal nature.

615. Subsection 3ZZUE(2) states that if the person is a natural person, the information, answer given or the fact that the person has given access to a document, and any information or thing that is obtained as a direct or indirect consequence, is not admissible in evidence against the individual except in a prosecution for providing false or misleading information or documents, or making a false document under Part 7.4 or 7.7 of the *Criminal Code*.

616. Subsection 3ZZUE(3) provides that nothing in any other law prevents an officer of the AFP from providing information to an inspecting officer in any form or from providing access to records of the AFP for the purposes of an inspection under this Division. This abrogation of the privilege against self-incrimination, subject to a use and derivative use immunity, recognises the public interest in the effective monitoring of the use of monitoring warrants to ensure that civil liberties are not unduly breached.

617. Subsection 3ZZUE(4) enables an officer of the AFP to make a record of information, or cause such a record to be made, for the purposes of giving the information to a person as permitted by subsection 3ZZUE(3), without being liable for a breach of any other law.

618. Subsection 3ZZUE(5) ensures that a claim for legal professional privilege over information, documents or other records provided or answers given under this clause is maintained.

**3ZZUF Exchange of information between Ombudsman and State or Territory inspecting authorities**

619. Section 3ZZUF allows the Commonwealth to develop effective and consistent inspection arrangements with other inspecting bodies, particularly state ombudsmen. Subsection 3ZZUF(4) provides definitions for 'State or Territory agency' and 'State or Territory inspecting authority' for the purposes of the section.

620. Subsection 3ZZUF(1) authorises the Ombudsman to give information that relates to a state or territory agency which was obtained by the Ombudsman under this Division to the state or territory inspecting authority responsible for inspecting that agency. Subsection 3ZZUF(2) requires that the Ombudsman be satisfied that it is necessary to give the information to the inspecting authority to enable it to perform its functions in relation to the state or territory agency.

621. Subsection 3ZZUF(3) empowers the Ombudsman to receive information relevant to the performance of the Ombudsman's functions under this Division from a state or territory inspecting authority.

**3ZZUG Ombudsman not to be sued**

622. Section 3ZZUG gives immunity from action, suit or proceeding to the Ombudsman, an inspecting officer or a person acting under an inspecting officer's direction or authority for an act or omission made in good faith in the performance or exercise, purported or otherwise, of a function, power or authority conferred under this Division. It further gives immunity to a Deputy Ombudsman or a delegate of the Ombudsman.

**3ZZUH Annual report**

623. Under this section, the Ombudsman is required to provide a written report to the Minister after the end of each financial year on the results of any inspections undertaken under section 3ZZUB. The note advises that this report will be included in the control orders annual report under section 104.29 of the *Criminal Code*. The Attorney-General must cause the control orders annual report to be tabled in both Houses of Parliament within 15 sitting days after the control orders annual report is complete.

624. Subsection 3ZZUH(2) requires the Ombudsman to include in the report the number of contraventions by the AFP and members and special members of the AFP of the provisions of Part IAAB or monitoring warrants identified by the Ombudsman in the year.

625. Subsection 3ZZUH(3) requires the Ombudsman to give a copy of a report under this section to the Commissioner and subsection 3ZZUH(4) provides that the report must not include information which, if made public, could reasonably be expected to endanger a person's safety, to prejudice an investigation, or prosecution, of an offence, or to compromise

the operational activities or methodologies of the AFP or any other Commonwealth, State, Territory or foreign law enforcement, intelligence or security agency.

***Criminal Code Act 1995***

**Item 2 – Subsection 104.29(1) of the *Criminal Code***

626. This item amends subsection 104.29(1).

627. Existing section 104.29 requires the Attorney-General to report annually on the operation of the control order regime in Division 104 of Part 5.3 of the *Criminal Code*.

628. This item amends section 104.29 by adding Division 5 of Part IAAB of the Crimes Act (monitoring warrants), and the rest of that Part of the Crimes Act to the extent that it relates to that Division. This amendment ensures that the Attorney-General's reporting requirements extend to the operation of the new monitoring warrant regime in Part IAAB of the Crimes Act, including any contraventions reported by the AFP Commissioner or the Commonwealth Ombudsman.

629. As already required by subsection 104.29(3), this report must be laid before each House of Parliament within 15 sitting days of that House after the report is completed.

**Item 3 – After paragraph 104.29(2)(f) of the *Criminal Code***

630. This item amends subsection 104.29(2) by inserting new paragraphs 104.29(2)(g)-(i). This amendment is incidental to the amendment to subsection 104.29(1) which extends the Attorney-General's reporting requirements to the new monitoring warrant regime in Division 5 of Part IAAB of the Crimes Act.

631. Existing subsection 104.29(2) deals with the matters that must be included in the Attorney-General's annual report on the operation of the control order regime in Division 104 of Part 5.3 of the *Criminal Code*. This amendment provides that the Minister must also include:

- the number of monitoring warrants issued under Division 5 of Part IAAB of the Crimes Act
- the number of warrants that were executed under that Division, and
- the report prepared by the Ombudsman under subsection 3ZZUH(1) of the *Crimes Act 1914* on the results of any inspections undertaken by the Ombudsman under section 3ZZUB .

632. These reporting obligations ensure the greatest transparency to the Parliament of the operation of the control order and monitoring warrants regime.

633. This item implements Recommendation 12 of the Committee advisory report.

## Schedule 9—Telecommunications interception

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

### Overview

634. Division 104 of Part 5.3 of the *Criminal Code* provides for the imposition of a range of obligations, prohibitions and restrictions on a person as part of a control order to prevent terrorism and hostile activities overseas. Commonwealth legislation confers a range of investigatory powers on law enforcement and other agencies. In particular, telecommunications interception warrants are currently available under the TIA Act for the purpose of investigating persons suspected of being involved in the commission of serious offences. However, neither the TIA Act nor other Commonwealth law provide adequate powers for law enforcement agencies to monitor compliance with controls under a control order to sufficiently reduce the risk that a person will engage in terrorist act planning or preparatory acts while subject to a control order.

635. The amendments in this Schedule will allow agencies to obtain warrants to monitor a person who is subject to a control order to protect the public from terrorist acts, prevent support for terrorist acts and hostile activities overseas, and to detect breaches of the order. Specifically, this regime will allow agencies to apply to an issuing authority for a TI warrant for the purposes of monitoring compliance with a control order issued under Division 104. It will also allow TI information to be used in any proceedings associated with that control order. The power to use telecommunications interception for monitoring purposes will remain a covert power. The amendments will introduce new deferred reporting arrangements, which will permit the chief officer of an agency to defer public reporting on the use of a warrant relating to a control order in certain circumstances, balancing the public interest in timely and transparent reporting with the public interest in preserving the effectiveness of this covert power.

636. The amendments will also permit the use of intercepted material in connection with PDOs to support a nationally-consistent prevention scheme.

### Item 1 – Subsection 5(1)

637. This item inserts new definitions of ‘confirmed control order’, ‘control order’, ‘engage in a hostile activity’, ‘foreign country’ and ‘interim control order’. These definitions have the meaning given in Part 5.3 of the *Criminal Code*.

638. This item inserts a new definition of ‘connected with’, defining when a purpose will be ‘connected with’ a ‘preventative detention order law’.

639. This item also inserts a new definition of ‘control order warrant’, providing a brief term describing warrants issued under new subsections 46(4) or 46A(2A).

640. In addition, this item inserts a definition of ‘control order warrant agency’. This definition is connected to item 13 which inserts new section 38A. This new section provides the Minister with the ability to amend a declaration under section 34 to authorise an eligible authority to apply for control order warrants under new subsections 46(4) and 46(2A).

**Item 2 – Subsection 5(1) (subparagraph (b)(vi) of the definition of *permitted purpose*)**

641. This item provides the AFP with the ability to use, communicate or record lawfully intercepted information for the purposes of a 'preventative detention order law'. This item is linked to the new definition of 'preventative detention order law' in item 5, which refers to Commonwealth, state and territory PDO regimes. By ensuring that the AFP can use, communicate and record such information in relation to all preventative detention frameworks, this item facilitates a nationally-consistent prevention scheme by removing a potential barrier to interoperability between the AFP and its state and territory counterpart agencies.

**Item 3 – Subsection 5(1) (at the end of paragraph (c) of the definition of *permitted purpose*)**

642. This item provides state and territory police with the ability to use, communicate or record lawfully intercepted information for the purposes of the Commonwealth control order regime (in Division 104 of the *Criminal Code*) and a 'preventative detention order law'.

643. Although the AFP is the only agency that can apply for a control order, the states and territories perform an enforcement role. As such, the state and territory police require the ability to use or to communicate lawfully intercepted information for the same purpose under Division 104 of the *Criminal Code*.

644. Lawfully intercepted information can already be used, communicated or recorded in relation to the Commonwealth PDO regime. As the PDO regime introduced in 2005 was designed to be a national scheme, this amendment is necessary to permit the use, communication and recording of lawfully intercepted information in relation to PDO regimes nationally. By ensuring that state and territory police forces can use, communicate and record such information in relation to all preventative detention frameworks, this item facilitates a nationally-consistent prevention scheme by removing a potential barrier to interoperability between the Commonwealth, state and territory agencies.

**Item 4 – Subsection 5(1) (definition of *preventative detention order*)**

645. This item repeals the definition of 'preventative detention order' in subsection 5(1) of the Act. This is a consequential amendment to the new definition of a 'preventative detention order law' in item 5.

**Item 5 – Subsection 5(1)**

*Definition of 'preventative detention order law'*

646. This item inserts a definition of 'preventative detention order law' into subsection 5(1) of the Act. This definition includes Commonwealth, state and territory PDO regimes.

*Definition of 'succeeding control order'*

647. This item inserts a definition of 'succeeding control order' into subsection 5(1) of the Act. A 'succeeding control order' has the meaning given in new section 6U of the Act, and is used as part of the test for a warrant relating to a control order under new subsections 46(4) and (5), and 46A(2A) and (2B). New subsection 57(6) also uses this defined term to permit a warrant to remain in force where a 'succeeding control order' exists.

*Definition of 'terrorist act'*

648. This item inserts a definition of 'terrorist act' into subsection 5(1) of the Act. A 'terrorist act' has the meaning given in Part 5.3 of the *Criminal Code*.

**Item 6 – Paragraph 5B(1)(bc)**

649. Item 6 amends the definition of 'exempt proceedings' in subsection 5B(1) of the Act to allow agencies to use lawfully intercepted information in a proceeding relating to Commonwealth, state and territory PDO regimes (within the meaning of the new definition of 'preventative detention order law' in item 5).

650. Lawfully intercepted information can already be used in a proceeding in relation to the Commonwealth PDO regime. As the Commonwealth PDO regime introduced in 2005 was designed to be a national scheme, this amendment is necessary to allow for lawfully intercepted information to be used in proceedings in relation to PDOs nationally. This will include applications for PDOs, in jurisdictions where applications are by way of proceeding, as well as a range of associated proceedings, such as appeals against and civil claims relating to PDOs.

**Items 7 and 8 – Section 6H**

651. These items amend section 6H of the Act to add references to new paragraphs inserted by later amendments to ensure the limitation on when an application for a warrant may be properly said to relate to a particular person also applies to warrants sought in connection with the operation of a control order.

**Item 9 – At the end of Part 1-2**

652. Item 9 inserts new sections 6T and 6U at the end of Part 1-2 of the Act.

653. The effect of new section 6T is to allow an application for a warrant relating to a control order to be made and issued prior to the control order being served on the person. This addresses the issue of an officer not being able to make an application for a warrant relating to a control order because the underlying control order has not come into force in accordance with section 104.5 of the *Criminal Code*.

654. This amendment is necessary to ensure that the interception warrant relating to the control order can operate from when the control order enters into force. Warrant applications and the subsequent process of provisioning an interception warrant can take a considerable period of time. If agencies were required to wait for a control order to be in force to apply for a warrant critical time may be lost to the time taken to then obtain and provision the warrant. The ability of an agency to deal in lawfully intercepted information that is obtained pursuant to a control order warrant prior to the entry into force of the relevant control order is subject to additional safeguards contained in new section 79AA.

655. New section 6U describes a successive control order in respect of the same person as a succeeding control order. Combined with the amendment at item 31 this ensures that a warrant relating to a control order continues to have effect once a 'succeeding control order' has been made in relation to a person.

**Item 10 – Subsection 7(9) (note)**

656. Item 10 repeals the existing note under subsection 7(9) and substitutes it with a new note that includes reference to the additional purpose for which interception warrants can be obtained, being purposes relating to a control order.

**Items 11, 12 and 13 – Control order warrants agency**

657. Section 5 of the Act contains a list of 'eligible authorities', being authorities of a state or territory that are eligible to be declared by the Minister under section 34 of the Act to be an 'interception agency', authorised to apply for and obtain interception warrants under Part 2-5 of the Act.

658. Section 35 of the Act establishes preconditions for the Minister to declare an eligible authority to be an interception agency. At present, paragraph 35(1)(a) requires the Minister to be satisfied that the law of the relevant state or territory makes satisfactory provision imposing on the chief officer of the eligible authority requirements corresponding to the requirements that sections 80 and 81 impose on the chief officer of a Commonwealth agency.

659. Items 38 and 39 amend the requirements contained in sections 80 and 81, to introduce new requirements relating to the control order warrant framework. Accordingly, item 12 amends the preconditions in paragraph 35(1)(a) relating to the record-keeping obligations in sections 80 and 81 of the Act to distinguish the existing requirements from the new record-keeping requirements in paragraphs 80(f) and (g) and 81(1)(h) relating to control order warrants (see items 38 and 39). The purpose of this amendment, in conjunction with item 13, is to ensure that an eligible authority is not precluded from being declared to be an interception agency, or cannot have its declaration revoked under section 37, should the law of the relevant state or territory not make satisfactory provision in relation to matters that relate exclusively to the control order warrant scheme.

660. Item 13 establishes the process for eligible authorities declared under section 34 of the Act to be made a 'control order warrant agency' (see item 1). The Minister can amend the declaration under section 34 if the Minister is satisfied that the law of the State makes satisfactory provision in regards to record-keeping, reporting and notification requirements relevant to control order warrants.

661. In the Committee advisory report, the Committee recommended (at Recommendation 11) that the AFP retain all relevant records in relation to the use of control order warrants and that the AFP notify the Commonwealth Ombudsman of the issuing of a control order warrant and of breaches of control order warrant requirements (see item 32). In addition, the Committee recommended that the Ombudsman report annually on the AFP's compliance with the control order warrant requirements (see items 46 and 47).

662. This Bill goes beyond Recommendation 11 of the Committee advisory report by applying these requirements to Commonwealth agencies and to state and territory interception agencies that wish to apply for control order warrants. Item 13 gives effect to this purpose by requiring states and territories to amend their legislation to make satisfactory provision of the control order warrant requirements that have been imposed on Commonwealth agencies. States and territories have been given an 18-month transitional period in which to amend their legislation should they wish for their agencies to continue to exercise the powers of a control order warrant agency (see item 59).

663. New subsection 38A(5) will require the Minister to remove the authorisation of an eligible authority to apply for control order warrants, if requested to do so by the Premier or Chief Minister of the relevant state or territory. New subsection 38A(6) will enable the Minister to amend a declaration under section 34 to remove an authorisation allowing an eligible authority to apply for control order warrants, if he or she is satisfied that the laws of a state or territory no longer make satisfactory provision of the particular requirements, or that the extent of compliance with the law of a relevant state or territory or the Act by an agency has been unsatisfactory. These provisions reflect the extant power of the Minister to revoke a declaration of an eligible authority, under section 37 of the Act.

664. However, unlike the revocation of a declaration, under section 37, an amendment to a declaration under subsections 38A(5) or (6) will be a legislative instrument.

665. New subsection 38A(7) provides that, if the Minister amends a declaration under subsections 38A(5) or (6) to remove an authorisation allowing an eligible authority to apply for control order warrants, the amendment does not affect the validity of a control order warrant issued before the amendment. This provision ensures that carriers, carriage service providers and agencies do not inadvertently engage in unlawful interception under a control order warrant issued to the relevant agency prior to the amendment, from the moment the amendment is made onwards, and that information obtained under such a warrant remains lawfully intercepted information.

**Items 14 and 15 – At the end of paragraphs 44A(2)(a) and (b)**

666. These items will allow the Victorian Public Interest Monitor to make submissions with respect to an application for an interception warrant relating to a control order under sections 46 and 46A, consistent with the Monitor's role in respect of other interception warrant applications under the Act.

**Items 16 and 17 – At the end of paragraph 45(2)(a) and (b)**

667. These items will allow the Queensland Public Interest Monitor to make submissions with respect to an application for an interception warrant relating to a control order under sections 46 and 46A, consistent with the Monitor's role in respect of other interception warrant applications under the Act.

**Items 18, 19 and 20 – Section 46**

668. These items amend section 46 to distinguish warrants issued in connection with the investigation of serious offences from warrants issued in relation to a person subject to a control order.

**Item 21 – At the end of section 46**

669. This item inserts three new subsections into section 46 in relation to the issue of telecommunications service warrants. These new subsections permit the issue of a telecommunications service warrant or 'B party' warrants relating to persons subject to a control order. A new heading of 'Control order warrant' has been included to distinguish this new type of warrant.

670. In considering an application for a control order warrant in relation to a telecommunications service under new subsection 46(4), the Judge or nominated AAT member must be satisfied that:

- Division 3 has been complied with in relation to the application
- in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone, and
- there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the service.

671. Before issuing a control order warrant, the Judge or nominated AAT member must be satisfied that information that would be likely to be obtained by intercepting under a warrant communications made to or from the telecommunications service would be likely to substantially 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
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

672. In addition, the Judge or nominated AAT member must be satisfied that he or she should issue the control order warrant, having regard to the following matters in subsection 46(5):

- how much the privacy of any person or persons would be likely to be interfered with by intercepting communications under a warrant
- how much the information obtained under the warrant would be 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, preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or determining whether the control order, or any succeeding control order, has been, or is being, complied with
- to what extent other methods have been used by, or are available to the agency
- how much the use of these alternative methods would be likely to assist the agency
- how much the use of these alternative methods would be likely to prejudice, whether because of delay or any other reason, the protection of the public from a terrorist act, preventing the provision of support for, or the facilitation of, a terrorist act, preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or determining whether the control order, or any succeeding control order, has been, or is being, complied with
- whether intercepting under a warrant communications made to or from the service would be the method likely to have the least interference with any person's privacy

- the possibility that the person in relation to whom the control order is in force has already engaged in this activity
- in relation to an application by an interception agency of Victoria—any submissions made by the Victorian PIM, and
- in relation to an application by an interception agency of Queensland—any submissions made by the Queensland PIM.

673. The underlying purpose of control orders and control order warrants is to prevent acts of terrorism and hostile activities. The requirement that the issuing authority have regard to the possibility of the person engaging in such conduct or breaching the control order is designed to ensure that the issuing authority has regard to evidence of both a specific risk or propensity of the person engaging in such conduct or breaching the order, as well as evidence that there is a general risk or propensity that the person will engage in such conduct or breach the control order. In making this decision, the issuing authority may consider a range of information, potentially including:

- whether there is specific or general evidence indicating that there is a possibility that the person may engage in the conduct the control order is intended to prevent, or may breach the control order
- evidence pre-dating the issuing or service of the control order, including the grounds on which the control order was issued, that may indicate such a possibility, notwithstanding the fact that the control order has subsequently been issued and/or served, and
- evidence about whether other persons subject to control orders have engaged in conduct the control order is intended to prevent, or have breached their control order, to the extent such evidence may indicate whether there is a possibility the person in question may engage in such conduct or breach the extant control order.

674. In essence, these cumulative factors require the issuing authority to undertake a proportionality test taking into consideration privacy concerns and the extent to which interception would assist in preventing terrorist and related acts or monitoring compliance with a control order.

675. The requirement for the issuing authority to have regard to whether intercepting under a warrant communications would be likely to have the least interference with any person's privacy implements Recommendation 13 of the Committee advisory report. The Committee's recommendation stated that the former Bill be amended to:

> explicitly require that the issuing officer is to have regard to whether the interception of telecommunications under the warrant constitutes the least interference with the liberty or privacy of any person that is necessary in all the circumstances.

676. New paragraph 46(5)(f) does not incorporate a requirement that the issuing authority have regard to whether the interception of communications constitutes the least interference with 'the liberty' of any person. The interception of communications (as a form of electronic surveillance) does not interfere with liberty, defined (relevantly) as 'freedom from control, interference, obligation, restriction, hampering conditions etc.; power or right of doing, thinking, speaking, etc., according to choice' or 'freedom from captivity, confinement or physical restraint' (Macquarie Dictionary Online) in a manner that is distinct from its

interference with privacy. As such, the inclusion of such a requirement in the context of interception (as distinct from the search warrant framework) would be without meaning.

677. New paragraph 46(5)(f) also does not explicitly incorporate the caveat contained in the Committee's recommendation that the issuing authority have regard to whether the relevant interference is 'necessary in all the circumstances'. Subsection 46(5) contains a detailed list of competing interests and considerations that issuing authorities must have regard to when determining whether they are satisfied that a control order warrant should be issued. This requirement approximates the effect of the caveat recommended by the Committee, and maintains consistency between the tests for a control order warrant and other interception warrants.

678. Subsection 46(6) places a restriction on the issuing of B-party warrants, which targets the telecommunications service of a person to whom the subject communicates. The issuing authority must not issue a B-party warrant over a telecommunications service unless he or she is satisfied that:

- the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person to whom the control order relates, or
- interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

**Items 22, 23 and 25 – Section 46A**

679. These items are designed to amend section 46A to distinguish warrants made in relation to serious offences from the new warrants made in relation to a person subject to a control order.

**Item 24 – After subsection 46A(2)**

680. This item inserts two new subsections into section 46A which concerns the issuing of named person warrants. Named person warrants enable all telecommunications services used or likely to be used by the person named in the warrant to be intercepted. These new subsections permit the issue of a named person warrant in relation to a person subject to a control order.

681. In considering an application for a control order warrant under new subsection 46A(2A), the Judge or nominated AAT member must be satisfied that information that would be likely to be obtained by intercepting communications made to or from a telecommunications service or telecommunications device would be likely to substantially 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
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

682. In addition, the Judge or nominated AAT member must have regard to the following matters in subsection 46A(2B):

- how much the privacy of any person or persons would be likely to be interfered with by intercepting communications under a warrant
- how much the information obtained under the warrant would be 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, preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or determining whether the control order, or any succeeding control order, has been, or is being, complied with
- to what extent other methods have been used by, or are available to the agency
- how much the use of these alternative methods would be likely to assist the agency
- how much the use of these alternative methods would be likely to prejudice, whether because of delay or any other reason, the protection of the public from a terrorist act, preventing the provision of support for, or the facilitation of, a terrorist act, preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country, or determining whether the control order, or any succeeding control order, has been, or is being, complied with
- whether intercepting under a warrant communications made to or from the service would be the method likely to have the least interference with any person's privacy
- the possibility that the person in relation to whom the control order is in force has engaged, provided, facilitated, or contravened with respect to the abovementioned activity, or is doing, or will do so in the future
- in relation to an application by an interception agency of Victoria—any submissions made by the Victorian PIM, and
- in relation to an application by an interception agency of Queensland—any submissions made by the Queensland PIM.

683. The underlying purpose of control orders and control order warrants is to prevent acts of terrorism and hostile activities. The requirement that the issuing authority have regard to the possibility of the person engaging in such conduct or breaching the control order is designed to ensure that the issuing authority has regard to evidence of both a specific risk or propensity of the person engaging in such conduct or breaching the order, as well as evidence that there is a general risk or propensity that the person will engage in such conduct or breach the control order. In making this decision, the issuing authority may consider a range of information, potentially including:

- whether there is specific or general evidence indicating that there is a possibility that the person may engage in the conduct the control order is intended to prevent, or may breach the control order
- evidence pre-dating the issuing or service of the control order, including the grounds on which the control order was issued, that may indicate such a possibility, notwithstanding the fact that the control order has subsequently been issued and/or served, and

- evidence about whether other persons subject to control orders have engaged in conduct the control order is intended to prevent, or have breached their control order, to the extent such evidence may indicate whether there is a possibility the person in question may engage in such conduct or breach the extant control order.

684. In essence, these cumulative factors require the issuing authority to undertake a proportionality test taking into consideration privacy concerns and the extent to which interception would assist in preventing terrorist and related acts or monitoring compliance with a control order.

685. The requirement for the issuing authority to have regard to whether intercepting under a warrant communications would be likely to have the least interference with any person's privacy implements Recommendation 13 of the Committee advisory report. The Committee's recommendation stated that the former Bill be amended to:

> explicitly require that the issuing officer is to have regard to whether the interception of telecommunications under the warrant constitutes the least interference with the liberty or privacy of any person that is necessary in all the circumstances.

686. New paragraph 46A(2B)(f) does not incorporate a requirement that the issuing authority have regard to whether the interception of communications constitutes the least interference with 'the liberty' of any person. The interception of communications (as a form of electronic surveillance) does not interfere with liberty, defined (relevantly) as 'freedom from control, interference, obligation, restriction, hampering conditions etc.; power or right of doing, thinking, speaking, etc., according to choice' or 'freedom from captivity, confinement or physical restraint' (Macquarie Dictionary Online) in a manner that is distinct from its interference with privacy. As such, the inclusion of such a requirement in the context of interception (as distinct from the search warrant framework) would be without meaning.

687. New paragraph 46A(2B)(f) also does not explicitly incorporate the caveat contained in the Committee's recommendation that the issuing authority have regard to whether the relevant interference is 'necessary in all the circumstances'. Subsection 46A(2B) contains a detailed list of competing interests and considerations that issuing authorities must have regard to when determining whether they are satisfied that a control order warrant should be issued. This requirement approximates the effect of the caveat recommended by the Committee, and maintains consistency between the tests for a control order warrant and other interception warrants.

**Item 26 – At the end of subsection 48(1)**

688. This item inserts a note that clarifies that only a control order warrant agency (see item 1) may apply for a control order warrant.

**Item 27 – At the end of subparagraph 48(3)(d)(ii)**

689. The purpose of section 48 is to allow agencies to enter premises and install equipment to intercept communications to or from a service when the interception by a carrier would be impractical or inappropriate.

690. This item permits the issue of a warrant authorising entry onto premises to effect interception in relation to a person subject to a control order where this is necessary for technical reasons, or to avoid jeopardising a purpose for which the warrant was obtained.

**Items 28, 29 and 30 – Section 49**

691. These items prescribe the form and content of the new warrants relating to a control order. New subsection 49(8) requires that a warrant relating to a person subject to a control order must:

- state that the warrant is issued on the basis of a control order made in relation to a person
- specify the name of the person
- specify the date the control order was made, and
- state whether the control order is an interim control order or a confirmed control order.

692. Items 28 and 29 amend section 49 to apply the existing requirements relating to the form and content of interception warrants to warrants relating to a person subject to a control order. These requirements include that the warrant must set out short particulars and that the warrant must specify the period for which it is to be in force; for instance, B-party warrants can only be effective for up to 45 days.

**Item 31 – At the end of section 57**

693. This item amends section 57 of the Act which relates to revocation of warrants by a chief officer, to apply to interception warrants issued in respect of a person subject to a control order. New subsection 57(6) provides that the chief officer of an agency must revoke a warrant relating to such a person if the control order or any succeeding control order has ceased to be in force.

**Item 32 – After section 59A**

694. The Committee advisory report recommended (at Recommendation 11) that the Bill be amended to require the AFP to notify the Commonwealth Ombudsman of the issuing of a control order warrant and of any breaches of the requirements of the control order warrant regime.

695. The Bill goes beyond the recommendation in the Committee advisory report, and imposes consistent notification obligations on all interception agencies, on the basis that if an agency has the ability to obtain a control order warrant, then the agency should be subject to the same oversight and accountability requirements as the AFP. For this reason, the Australian Crime Commission (ACC), Australian Commission for Law Enforcement Integrity (ACLEI) and the AFP (as each are within the definition of 'Commonwealth agency' in section 5) must adhere to the notification requirements in new section 59B.

**Item 33 – Subsections 63(1) and (2)**

696. This item amends section 63 of the Act, which prohibits dealing in lawfully intercepted information or interception warrant information. This amendment ensures that the prohibition on dealing with intercepted information is subject to the operation of new section 299, which permits limited use of information obtained under a warrant relating to an interim control order which is subsequently declared void (see item 58).

**Item 34 – Section 65A**

697. This item replaces section 65A of the Act to allow an employee of a carrier to communicate lawfully intercepted information and interception warrant information for purposes connected with the investigation by an agency of a serious offence and for purposes connected with a control order warrant.

**Item 35 – Section 67**

698. This item amends section 67 of the Act to ensure that lawfully intercepted information obtained under a control order warrant can be used, communicated or recorded for purposes connected with monitoring compliance with the control order and associated purposes (including protecting the public from a terrorist act and in connection with PDOs).

**Items 36 and 37 – Sections 79 and 79AA**

699. Item 37 inserts a new section 79AA, which provides that information obtained under a warrant relating to a control order that was issued prior to the control order coming into force must be destroyed if the sole purpose, or one of the purposes, of issuing the warrant was to determine whether the person would comply with the control order (or any succeeding control order). This destruction requirement applies unless the chief officer is satisfied that the information is likely to assist in connection with the following matters:

- 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 the facilitation of, the engagement in a hostile activity in a foreign country.

700. This amendment ensures agencies can only use information intercepted for the purposes of monitoring compliance with a control order for limited purposes associated with protecting the public from a terrorist act.

701. Subsection 79AA(2) removes application of section 6T, which would otherwise operate to provide that a control order is in force notwithstanding it has not been served on the subject. The subsection ensures the limitation is effective to prevent the use of communications intercepted prior to the control order being served on the subject.

702. Item 36 amends the heading to section 79 of the Act in light of the insertion of section 79AA.

**Item 38 – At the end of section 80**

703. Item 38 establishes a record-keeping obligation on agencies to keep advice given by the chief officer to defer the publication of control order information. In addition, new paragraph (g) requires agencies to retain the decision of the Minister on whether to include the information in the report.

**Item 39 – After paragraph 81(1)(g)**

704. Pursuant to new subsection 103B(4), the chief officer of an agency must reconsider previous advice to defer the publication of control order information to determine whether the

information should be included in the next Ministerial report. This item creates a record-keeping obligation in relation to that reconsideration by the chief officer where in the opinion of the chief officer the information remains 'control order information' for the purposes of section 103B.

**Items 40 and 41 – Section 81A**

705. In accordance with section 81A, the Secretary of the Commonwealth Attorney-General's Department is required to keep a General Register in relation to each Part 2-5 warrant including their particulars (e.g. the date of issue of the warrant, the issuing authority who issued the warrant and the agency to which the warrant was issued).

706. These items amend section 81A to require that particulars of interception warrants relating to a person subject to a control order are kept in the General Register of Warrants.

**Items 42 and 43 – Section 81C**

707. In accordance with section 81C, the Secretary of the Commonwealth Attorney-General's Department is required to keep a Special Register in relation to each registrable expired warrant including their particulars (e.g. the date of issue of the warrant, the issuing authority who issued the warrant and the agency to which the warrant was issued).

708. These items amend section 81C to require that particulars of interception warrants relating to a person subject to a control order are kept in the Special Register of Warrants.

**Items 44 and 45 – Ombudsman inspections**

709. These items are in response to Recommendation 11 of the Committee advisory report, which recommended that the Ombudsman report to the Attorney-General annually regarding the AFP's compliance with the requirements of the control order warrant regime.

710. Similar to the approach taken to item 32, above, the Bill goes beyond the recommendation of the Committee, and introduces a consistent oversight framework for all interception agencies, on the basis that if an agency has the ability to obtain a control order warrant, then the agency should be subject to the same oversight and accountability requirements as the AFP.

711. Accordingly, item 44 expands the Ombudsman's inspection regime to include new section 79AA, which requires that information received before a control order comes into force be destroyed unless the information is likely to assist in connection with a prescribed purpose (see items 36 and 37).

712. Item 45 allows the Ombudsman to inspect a Commonwealth agency's records, to the extent of their compliance with the provisions in new subsection 59B(2), if the Ombudsman has received notification from a chief officer of a Commonwealth agency that an officer has contravened a provision in new subsection 59B(2) and the contravention occurred in that period.

**Items 46 and 47 – Ombudsman reports**

713. Item 46 is a consequential amendment to item 45, where the Ombudsman can conduct an inspection following notification of a contravention of certain requirements (as found in

subsection 59B(2)). This item amends section 84 to allow the Ombudsman to include the results of such an inspection in its report for that financial year.

714. Item 47 inserts section 85A, which applies to the situation in which the chief officer of an agency has notified the Ombudsman that an officer has contravened a certain requirement (in subsection 59B(2)) and the Ombudsman decides not to conduct an inspection as a result. Pursuant to new section 85A, the Ombudsman can report on notifications received without conducting an inspection in direct response to each notification under subsection 83(3).

**Item 48 – Subparagraph 103(ae)(i)**

715. Item 48 amends subparagraph 103(ae)(i) of the Act, to enable the Minister to include a summary of any information that is included in the Ombudsman's report under subsection 84(1), as opposed to information that is required to be included in such reports under subsection 84(1A), in his or her report that is tabled in the Parliament in accordance with sections 99 and 104 of the Act. This amendment ensures that information that is included in such reports pursuant to new section 85A of the Act may be included in the Minister's report when it is tabled in the Parliament.

**Item 49 – At the end of Division 2 of Part 2-8**

716. This item inserts a new section 103B, which allows for the public reporting of control order warrants (including breaches in relation to those warrants) to be deferred until a subsequent report in limited circumstances. Under subsection 103B(2), the chief officer of a Commonwealth agency or the chief officer of an eligible authority of a State must advise the Minister not to include the information in the Minister's report, which is tabled in Parliament, if the chief officer is satisfied that the information is 'control order information' as defined in new subsection 103B(6). This 'control order information' is information, if made public, could reasonably be expected to enable a reasonable person to conclude that:

- a control order warrant is likely to be, or is not likely to be, in force in relation to a telecommunications service used, or likely to be used, by a particular person, or
- a control order warrant is likely to be, or is not likely to be, in force in relation to a particular person.

717. Pursuant to subsection 103B(3) the Minister can act on the advice of the chief officer of the agency and not include the information in the report. If this is the case, there remains a positive obligation on the chief officer of the agency to advise the Minister to include the information in the next report if the chief officer is satisfied that a reasonable person could no longer draw those inferences from the information.

718. The reason for this new section is that control orders have historically been sought and made only rarely with the effect that it is uncommon for there to be more than a limited number of control orders in force at any given time. If the Minister were required to contemporaneously publicly report on control order warrants, and only a limited number of persons are subject to control orders at that time, annual reporting may effectively reveal that a particular person who is subject to a control order is or is not also subject to covert surveillance.

719. The ability of a person to determine, or to speculate with a degree of certainty, whether they are, or are not, likely subject to interception may be further enhanced if the relevant control order contains particular conditions or restrictions that are particularly amenable to monitoring by way of telecommunications interception. This would undermine the purpose and effectiveness of such warrants, by enabling and incentivising persons to either adopt counter-measures to avoid or reduce the effectiveness of covert surveillance (if the person determines they are, or are likely to be, under surveillance), or to breach the terms of the control order or engage in serious malfeasance (if the person determines they are not, or are unlikely to be, under surveillance).

**Item 50 – At the end of subsection 133(2)**

720. This item amends section 133 of the Act, which prohibits dealing with lawfully accessed information. This amendment ensures that the prohibition on dealing with lawfully accessed information is subject to the operation of new section 299, which allows for the limited use of information obtained under a warrant relating to an interim control order which is subsequently declared void (see item 58).

**Items 51, 52, 53, 54 and 55 – New section 139B**

721. Item 53 inserts new section 139B which ensures that lawfully accessed information can be used, communicated or recorded for a purpose connected with Division 104 of the *Criminal Code* or a 'preventative detention order law'.

722. This amendment to the dealing provisions of the stored communications regime in the Act is necessary because, under a telecommunications interception warrant, agencies are able to lawfully access stored communications. Accordingly, this amendment allows agencies to use, communicate or record this information in relation to the control order regime and Commonwealth, state and territory PDO regimes.

**Item 56 – Chapter 6 (heading)**

723. This item amends the heading to Chapter 6 to 'Miscellaneous' because this chapter no longer applies solely to regulations (see item 58).

**Item 57 – Part 6-1 (heading)**

724. The heading to Part 6-1 has been amended to 'Miscellaneous' because this chapter no longer applies solely to regulations (see item 58).

**Item 58 – Before section 300**

725. This item inserts section 298 which provides protection from prosecution for persons who act in good faith in the execution of a warrant or the performance of a related function or duty where the interim control order underlying the issue of the warrant is later declared void.

726. Pursuant to Division 104 of the *Criminal Code*, the AFP can apply to an issuing court to make an interim control order with respect to a person. If the interim control order is made, the AFP can then elect to confirm the control order at a confirmation hearing in court. This amendment addresses the potential for warrants relating to a control order to be executed and acted upon prior to the control order being declared void at the confirmation hearing.

727. New section 298 provides that a person is immune from criminal liability for anything done, or omitted to be done, in good faith before the control order was declared void in the purported execution of a control order warrant, or the purported exercise of a power or performance of a function or duty that is consequential on the warrant.

728. This qualified immunity from criminal prosecution recognises the inherent risks assumed by law enforcement officers and persons assisting them in relying in good faith on legal authorities that may subsequently be declared void *ab initio*. Importantly, this qualified immunity does not:

- protect persons from criminal liability for acts done, or omitted to be done, otherwise than in good faith
- protect persons from criminal liability for acts done, or omitted to be done, subsequent to a control order being declared void (if, at the time, the person knew, or ought reasonably to have known, of the declaration), or
- protect law enforcement agencies from civil liability in these circumstances.

729. This item also inserts section 299 which allows for the limited use of either lawfully intercepted information or lawfully accessed information obtained under a warrant relating to an interim control order which is subsequently declared void. The information may be used, communicated, recorded or given in evidence in a proceeding when it is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, serious damage to property or a purpose connected with a Commonwealth, state or territory PDO regime.

730. This provision is intended to address the unlikely scenario where:

- an interim control order has been issued in respect of a person;
- a law enforcement agency has duly obtained a control order warrant in relation to that person;
- under that control order warrant, the agency has obtained information that indicates that the person is likely to engage in a terrorist act, cause serious harm to a person, or cause serious damage to property;
- before the agency can act on that information, the interim control order is considered by a court at a confirmation hearing and declared void *ab initio* pursuant to subsection 104.14(6) of the *Criminal Code* on the grounds that, at the time of making the interim control order, there were no grounds on which to make the order.

731. As the existence of a valid control order is a condition for the issuing of a control order warrant, the likely effect of a court declaring an interim control order void *ab initio* pursuant to subsection 104.14(6) of the *Criminal Code* would be that any control order warrants predicated on that control order would also likely be void *ab initio*.

732. It is a fundamental principle of the Australian legal system that courts have a discretion as to whether or not information may be admitted as evidence into proceedings, irrespective of the manner in which the information was obtained. As an example, the

*Bunning v Cross*[11] discretion places the onus on the accused to prove misconduct in obtaining certain evidence and to justify the exclusion of the evidence. This principle is expanded on in Commonwealth statute[12], where there is an onus on the party seeking admission of certain evidence to satisfy the court that the desirability of admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. This fundamental principle reflects the need to balance the public interest in the full availability of relevant information in the administration of justice against competing public interests, and demonstrates the role the court plays in determining admissibility of evidence.

733. However, the TIA Act departs from these fundamental principles, by imposing strict prohibitions on when material under the Act may be used, communicated or admitted into evidence.[13] Under the TIA Act, it is a criminal offence for a person to deal in information obtained under the Act for any purpose, unless the dealing is expressly permitted under one or more of the enumerated and exhaustive exceptions to the general prohibition. This prohibition expressly overrides the discretion of the judiciary, both at common law and under the Evidence Act, to admit information into evidence where the public interest in admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. There is also a risk that the prohibition might be interpreted, either by a court considering the matter after-the-fact, or by an agency considering the question *in extremis*, to override the general defence to criminal responsibility under the *Criminal Code*.

734. For this reason, the Bill will insert section 299 to the TIA Act, which would expressly permit agencies to rely on such information to prevent, or lessen the risk, of a terrorist act, serious harm to a person, or serious damage to property. This provision will also permit such information to be used to apply for, and in connection with, a PDO.

**Part 2—Transitional Provisions**

**Item 59 – Agencies authorised to apply for control order warrants**

735. Item 59 is a transitional provision. Subitem (2) deems all pre-existing declarations in relation to eligible authorities to be taken to authorise the respective eligible authority to apply for control order warrants. The intended effect of this item is that state and territory police forces and other eligible authorities listed in section 5 of the Act (all of which have been declared under section 34) will be permitted to apply for control order warrants from the commencement of Schedule 9.

736. Subitem (3) allows state and territory Parliaments 18 months following the commencement of Schedule 9 to amend their laws to implement the control order requirements in new subsection 38A(4). The requirements set out in new section 38A go beyond the safeguards recommended by the Committee. The control order warrant scheme is intended to mitigate the risk of terrorism in an elevated threat environment. These provisions will allow state and territory agencies responsible for counter-terrorism efforts to effectively monitor those subject to a control order from commencement and allow state and territory Parliaments time to consider legislation to give effect to these additional safeguards.

---

[11] (1978) 141 CLR 54.
[12] Section 138 of the *Evidence Act 1995 (Cth)*.
[13] See section 63 of the TIA Act.

**Item 60 – Validation of dealing with information – preventative detention orders**

737. This amendment is to ensure that an officer or staff member of a state or territory agency who previously communicated, made use of, or made a record of lawfully intercepted information for a purpose subsequently covered by the amended definition to 'permitted purpose' (see item 3), or a person who gave or admitted evidence in a proceeding subsequently covered by the amended definition to 'exempt proceeding' (see item 6) would be taken not to have contravened the prohibitions under section 63 of the Act. Paragraph (2)(d) is intended to ensure that the item does not interfere with any past decision of a court, tribunal or other body or person to exclude such evidence.

738. There is a clear parliamentary intent to make lawfully intercepted information obtained under the TIA Act available for the purposes of identifying, preventing and prosecuting acts of terrorism. This is reflected in the purposes for which lawfully intercepted information can be used, communicated, recorded and admitted into evidence in the TIA Act.

739. The PDO regime was established in 2005 based on a Council of Australian Governments agreement. The intention was for this to become a seamless national regime.

740. However, there is an anomaly in the TIA Act, which only allows lawfully intercepted information to be made available for the Commonwealth PDO regime.

741. This anomaly has only been discovered as a result of recent operational activities and because of differences in the operation of PDO regimes at the state and territory and Commonwealth level. These subtle differences have resulted from the implementation of the PDO regimes between jurisdictions. At the Commonwealth level, and in a number of states and territories, applications for PDOs are made to issuing authorities, who serve in their personal capacities, similar to an application for a warrant. In other jurisdictions, applications are made to a court, similar to applications for control orders. While subtle, this distinction has important implications for the operation of the TIA Act, which contains distinct rules for when lawfully intercepted information may be disclosed to a person (such as an issuing authority), and when it may be given and adduced into evidence in court. This amendment is designed to rectify this irregularity.

**Schedule 10—Surveillance devices**

***Surveillance Devices Act 2004***

**Overview**

742. Division 104 of Part 5.3 of the *Criminal Code* provides for the imposition of a range of obligations, prohibitions and restrictions on a person as part of a control order to prevent terrorism and hostile activities overseas. Commonwealth legislation confers a range of investigatory powers on law enforcement and other agencies. In particular, the existing surveillance device warrant regime is only available where the issuing authority is satisfied that one or more relevant offences have been, are being, are about to be, or are likely to be, committed. However, neither the SD Act nor other Commonwealth law provide adequate powers for law enforcement agencies to monitor compliance with controls under a control order to sufficiently reduce the risk that a person will engage in terrorist act planning or preparatory acts while subject to a control order.

743. The amendments in this Schedule will allow agencies to obtain warrants to monitor a person who is subject to a control order to detect breaches of the order. Specifically, this regime will allow law enforcement officers to apply to an issuing authority for a surveillance device warrant for the purposes of monitoring compliance with a control order issued under Division 104. It will allow surveillance device information to be used in any proceedings associated with that control order. It will also extend the circumstances in which agencies may use less intrusive surveillance devices without a warrant to include monitoring of a control order, and will allow protected information obtained under a control order warrant to be used to determine whether the control order has been complied with. The power to use surveillance devices for monitoring purposes will remain a covert power. The amendments will introduce new deferred reporting arrangements, which will permit the chief officer of an agency to defer public reporting on the use of a monitoring warrant in certain circumstances, balancing the public interest in timely and transparent reporting with the public interest in preserving the effectiveness of this covert power.

**Item 1 – After paragraph 3(a)**

744. This item amends section 3 of the SD Act, which sets out the main purposes of the Act, to insert new paragraphs 3(aa) and 3(ab). These paragraphs reflect the amendments contained in this Schedule, which enable law enforcement officers to obtain surveillance device warrants and tracking device authorisations where a control order is in force in relation to a person to assist in the protection of the public, the prevention of support for terrorist acts or engagement in a hostile activity in a foreign country, or monitoring compliance with the control order.

**Item 2 – At the end of section 4**

745. This item amends section 4, which clarifies the relationship between the Act and other Commonwealth, state and territory laws, and other matters, to insert new subsections 4(5) and (6). The new subsections clarify that a warrant may be issued, or a tracking device authorisation made, under the Act for the purposes of:

(i) protecting the public from a terrorist act; or

(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with.

**Item 3, 4, 5, and 6 – Subsection 6(1)—Definitions**

746. Item 3 inserts additional definitions relevant to control orders and PDOs.

747. Under the new definitions the terms ‘confirmed control order’, ‘control order’, ‘engage in a hostile activity’, ‘foreign country’ and ‘interim control order’ take the meanings given in Part 5.3 of the *Criminal Code*.

748. The new definition of ‘control order information’ is relevant to new section 50A under which an agency can advise the Minister to defer reporting of such information.

749. The new definition of 'control order warrant' provides that it means a surveillance device warrant issued in response to an application by a law enforcement officer under new subsection 14(3C), which permits the issue of a surveillance device warrant where a control order is in force and the issue of the warrant would assist in the protection of the public, the prevention of terrorist related acts or engagement in hostile activities in a foreign country, or monitoring compliance (see Item 8).

750. The term 'foreign country' when used in the expression 'hostile activity in a foreign country', has the meaning given in Part 5.3 of the *Criminal Code*.

751. This item also inserts a definition of 'preventative detention order law' into subsection 6(1) of the Act. This definition includes Commonwealth, state and territory PDO regimes.

752. Items 4 and 5 amend the existing definition of 'relevant proceeding' to include proceedings arising under Divisions 104 (control orders) of the *Criminal Code*, or relating to a matter arising under a 'preventative detention order law' (see item 3). The effect of these amendments is to permit protected information to be used, recorded, communicated or published, or admitted into evidence under section 45(5) of the Act if it is necessary for the purposes of one or more of these proceedings.

753. Item 6 inserts new definitions of 'succeeding control order' and 'terrorist act'. Succeeding control order has the same meaning given by section 6D. Terrorist act has the meaning given in Part 5.3 of the *Criminal Code*.

**Item 7 – After section 6B**

754. Item 7 inserts a new section 6C, which allows an application for a control order warrant to be made and a warrant to be issued prior to the control order having been served on the person under Division 104 of the *Criminal Code*. This amendment is necessary to ensure that the surveillance device warrant relating to the control order can operate from when the control order enters into force. Warrant applications and the subsequent process of provisioning a surveillance device warrant can take a considerable period of time. If agencies were required to wait for a control order to be in force to apply for a warrant critical time may be lost to the time taken to then obtain and provision the warrant. In particular, this provision is designed to ensure that officers have an opportunity to install surveillance devices covertly, as there are often limited opportunities to do so.

755. Section 6D provides that any successive control order made in relation to the same person is termed a 'succeeding control order'. The concept of a succeeding control order is intended to reflect the fact that, under Division 104 of the *Criminal Code*, an initial interim control order may be succeeded by a confirmed control order, which in turn may be succeeded by one or more subsequent control orders. In each case, the preceding control order ceases to be in force and a new, succeeding control order enters into force. The definition of succeeding control order is used throughout the new control order monitoring provisions to ensure that control order warrants and tracking device authorisations may be issued or given, and information obtained via the use of those powers may be dealt with, in connection with any one or more of that potential series of control orders, rather than being limited to the specific control order that is in force at a given point in time.

**Item 8 – After subsection 14(3B)**

756. Item 8 inserts new subsection 14(3C) which establishes the application process for a control order warrant. A law enforcement officer (or person on their behalf) may apply for the issue of a control order warrant if a control order is in force (whether or not, within the meaning of new section 6C, it has been serviced on the person) and the officer suspects, on reasonable grounds, that the use of a surveillance device to obtain information relating to the person subject to the control order would be likely to substantially assist in:

- protecting the public from a terrorist act; or
- preventing the provision of support for, or the facilitation of, a terrorist act; or
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

**Item 9 – Subsection 14(4)**

757. Item 9 omits 'or (3B)' from subsection 14(4) of the Act and replaces it with '(3B) or (3C)'. Subsection 14(4) of the Act deals with the procedure for making applications for a surveillance device warrant, namely that an application can be made to an eligible Judge or nominated AAT member. This amendment to subsection 14(4) of the Act allows applications for control order warrants under the new subsection 14(3C) of the Act to be made to an eligible Judge or nominated AAT member.

**Item 10 – Paragraph 14(6)(a)**

758. Subsection 14(6) allows a law enforcement officer to apply for a surveillance warrant without an affidavit in limited circumstances. This item amends paragraph 14(6)(a) to enable a law enforcement officer to apply for a surveillance device warrant without an affidavit when the immediate use of a surveillance device would be likely to substantially assist in:

- protecting the public from a terrorist act; or
- preventing the provision of support for, or the facilitation of, a terrorist act; or
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

**Item 11 – After paragraph 16(1)(bb)**

759. Subsection 16(1) establishes the factors that an eligible Judge or nominated AAT member must be satisfied of when determining whether to issue a surveillance device warrant.

760. This item inserts a new paragraph (bc) to subsection 16(1) of the Act to provide that the eligible Judge or AAT member may issue a surveillance device warrant only if satisfied

that a control order is in force in relation to the person, and that the use of a surveillance device to obtain information relating to the person would be likely to substantially assist in:

- protecting the public from a terrorist act; or
- preventing the provision of support for, or the facilitation of, a terrorist act; or
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

761. The reference to a control order being in force when issuing the surveillance device warrant under subsection 16(1) includes an interim control order or confirmed control order as defined under subsection 6(1). It also includes a control order that is in force under subsection 6C even if it has not yet been served on the person.

**Item 12 – At the end of subsection 16(1)**

762. This item adds a note that refers to section 6C, which provides that control orders that have been made but not come into force within the meaning of Division 104 of the *Criminal Code* are deemed to be in force for the purposes of the Act. For the purposes of making and determining an application for a control order warrant, this has the effect of allowing a control order warrant to be issued prior to the service of the control order on the person.

**Item 13, 14 and 15 – Subsection 16(2)**

763. Subsection 16(2) of the Act lists matters that an eligible Judge or nominated AAT member must have regard to when determining whether a surveillance device warrant should be issued.

764. Item 13 inserts paragraphs 16(2)(eb), (ec) and (ed) into subsection 16(2) of the Act. The intention of these paragraphs is to ensure that in determining whether a control order warrant should be issued the issuing authority has regard to the likely value of information sought to be obtained, and the possibility that a person has or will engage in, facilitate or provide support for a terrorist act, or hostile activity in a foreign country, or has or will contravene a control order. In response to Recommendation 14 of the Committee advisory report, the issuing authority must have regard to whether the use of the surveillance device in accordance with the warrant would be likely to have the least interference with any person's privacy.

765. The underlying purpose of control orders and control order warrants is to prevent acts of terrorism and hostile activities. The requirement that the issuing authority have regard to the possibility of the person engaging in such conduct or breaching the control order is designed to ensure that the issuing authority has regard to evidence of both a specific risk or propensity of the person engaging in such conduct or breaching the order, as well as evidence that there is a general risk or propensity that the person will engage in such conduct or breach the control order. In making this decision, the issuing authority may consider a range of information, potentially including:

- whether there is specific or general evidence indicating that there is a possibility that the person may engage in the conduct the control order is intended to prevent, or may breach the control order
- evidence pre-dating the issuing or service of the control order, including the grounds on which the control order was issued, that may indicate such a possibility, notwithstanding the fact that the control order has subsequently been issued or served, and
- evidence about whether other persons subject to control orders have engaged in conduct the control order is intended to prevent, or have breached their control order, to the extent such evidence may indicate whether there is a possibility that the person in question may engage in such conduct or breach the extant control order.

766. As noted above, the requirement for the issuing authority to have regard to whether the use of a surveillance device in accordance with the warrant would be likely to have the least interference with any person's privacy implements Recommendation 14 of the Committee advisory report. The Committee's recommendation stated that the former Bill be amended to:

> explicitly require that the issuing officer is to have regard to whether the use of the surveillance device under the warrant constitutes the least interference with the liberty or privacy of any person that is necessary in all the circumstances.

767. New paragraph 16(2)(ec) does not incorporate a requirement that the issuing authority have regard to whether the use of the surveillance device constitutes the least interference with 'the liberty' of any person. Covert surveillance does not interfere with liberty, defined (relevantly) as 'freedom from control, interference, obligation, restriction, hampering conditions etc.; power or right of doing, thinking, speaking, etc., according to choice' or 'freedom from captivity, confinement or physical restraint' (Macquarie Dictionary Online) in a manner that is distinct from its interference with privacy. As such, the inclusion of such a requirement in the context of surveillance (as distinct from the search warrant framework) would be without meaning.

768. New paragraph 16(2)(ec) also does not explicitly incorporate the caveat contained in the Committee's recommendation that the issuing authority have regard to whether the relevant interference is 'necessary in all the circumstances'. Subsection 16(2) contains a detailed list of competing interests and considerations that issuing authorities must have regard to when determining whether they are satisfied that a control order warrant should be issued. This requirement approximates the effect of the caveat recommended by the Committee, and maintains consistency between the tests for a control order warrant and other surveillance device warrants.

769. The purpose of item 14 is to limit the application of paragraph 16(2)(f) to apply only to applications for warrants in relation to a relevant offence or recovery order. The consideration of whether a previous control order warrant was sought or issued in relation to a person is dealt with under paragraph 16(2)(g).

770. Item 15 inserts a new provision to require an eligible Judge or nominated AAT member to have regard to any previous control order warrant sought or issued on the basis of a control order relating to the person.

**Item 16 – After subsection 17(1)**

771. New section 17 sets the content requirements for a surveillance device warrant, which includes amongst other things, the name of the applicant and the kinds of surveillance devices authorised to be used under the warrant. This requirement ensures that the warrant clearly states its scope.

**Item 17 – Subsection 20(2)**

772. Subsection 20(2) sets out circumstances in which a chief officer of a law enforcement agency must revoke a surveillance device warrant.

773. Item 17 amends s 20(2) to extend the circumstances in which the chief officer of a law enforcement agency must revoke a warrant to include the circumstances set out in new paragraphs 21(3C)(a) and (b) and 21(3D)(a) and (b), which relate to control order warrants (see Item 18).

**Item 18 – After subsection 21(3B)**

774. Section 21 sets out the circumstances in which the chief officer of a law enforcement agency is required to revoke a warrant under section 20 and to ensure that the use of surveillance devices authorised by the warrant is discontinued.

775. Item 18 inserts subsections 21(3C) and 21(3D) to the Act. These new subsections provide that, where the chief officer is satisfied that the use of a surveillance device under a control order warrant is no longer required for the purposes indicated in paragraph 21(3C)(b), or that no control order is in force, the chief officer must revoke the warrant under subsection 20(2) and take steps necessary to ensure the use of surveillance devices under that warrant is discontinued as soon as practicable. This requirement is intended to minimise the interference with the privacy of any persons associated with the use of surveillance devices under a control order warrant.

776. The requirement for the chief officer to ensure that the use of surveillance devices is discontinued 'as soon as practicable' reflects that discontinuing the use of a surveillance device can, in some cases, require the covert deactivation and recovery of a device installed on or in a premises or object. Agencies may need to wait for an appropriate opportunity to do so in some circumstances.

**Item 19 – At the end of section 37**

777. Section 37 of the Act allows limited use of an optical surveillance device without a warrant where it will not involve entry onto premises without permission or interference without permission with any vehicle or thing.

778. Item 19 inserts the new subsection 37(4) providing that law enforcement officers of state and territory police acting in the course of their duties may also use an optical surveillance device without a warrant to obtain information about the activities of the person subject to a control order, for the purposes of:

- protecting the public from a terrorist act; or
- preventing the provision of support for, or the facilitation of, a terrorist act; or

- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

779. The use of optical surveillance devices by Commonwealth law enforcement officers without a warrant for comparable purposes is covered under the existing subsection 37(1).

**Items 20 and 21 – Section 38**

780. Section 38 of the Act permits Commonwealth, state and territory law enforcement officers to use a surveillance device to listen to or record words spoken without a warrant in limited circumstances. It also allows for non-law enforcement officers assisting a Commonwealth, state and territory law enforcement officer to do so.

781. New subsection 38(3A) allows a state or territory law enforcement officer to use a surveillance device without a warrant to obtain information relating to a person subject to a control order, in limited circumstances.

782. Similarly, the new subsection 38(6) allows for a person assisting a state or territory law enforcement officer to use a surveillance device without a warrant to obtain information relating to a person subject to a control order in limited circumstances.

**Item 22 – After subsection 39(3A)**

783. Item 22 inserts a new subsection 39(3B) to the Act to permit a law enforcement officer to use a tracking device, with the written permission of an appropriate authorising officer, for obtaining information relating to a person who is subject to a control order for the purposes of:

- protecting the public from a terrorist act; or
- preventing the provision of support for, or the facilitation of, a terrorist act; or
- preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- determining whether the control order, or any succeeding control order, has been, or is being, complied with.

784. Subsection 39(3B) is subject to the limitation under subsection 39(8), which provides that an appropriate authorising officer must not give permission for the use, installation or retrieval of a tracking device, if its use or retrieval involves entry on to premises without permission or interference with the interior of a vehicle without permission.

**Items 23 and 24 – Section 39**

785. Item 23 is a consequential amendment to substitute references to subsections '39(1), (3) and (3A)' of the Act with references to subsections '39(1), (3), (3A) and (3B)' to ensure that provisions relating to tracking devices also apply to tracking device authorisations given in relation to a person subject to a control order.

786. Item 24 is a consequential amendment, substituting references in subsections 39(5) and (7) to 'subsections 39(1), (3) and (3A)' with references to 'subsections 39(1), (3), (3A) and (3B)'. The effect of these amendments is to ensure that multiple tracking devices can be used under a tracking device authorisation given in relation to a person subject to a control order, and that any such authorisation (or retrieval authorisation) must indicate the period, not exceeding 90 days, for which the authorisation remains in force.

**Item 25 – After paragraph 40(1)(da)**

787. Section 40 of the Act requires the appropriate authorising officer, who has given their permission for the use of a tracking device without a warrant under section 39, to make a written record of giving the authorisation as soon as practicable after giving the authorisation. The record is to contain the matters listed in paragraphs 40(1)(a) to (k).

788. Item 25 inserts a new paragraph 40(1)(db) to require that, in relation to a tracking device authorisation given in relation to a person subject to a control order, the matters which are to be recorded must also include details identifying the name of the person, the date the control order was made, and whether the control order is an interim control order or a confirmed control order.

**Items 26, 27, 28, 29, 30 and 31 – Section 45**

789. Section 45 of the Act creates offences with respect to the unlawful use, recording, communication, or publication of 'protected information'. Protected information is defined in section 44 of the Act.

790. Subsection 45(1) of the Act makes it an offence to use, record, communicate or publish any information, when that information falls within the definition of protected information and such use is not permitted by one of the exceptions. Subsection 45(2) of the Act makes it an aggravated offence if a person uses, records, communicates or publishes protected information in a manner that endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence.

791. Item 26 and 27 are consequential amendments and insert 'or section 65B (which deals with information obtained before an interim control order is declared void)' to paragraphs 45(1)(c) and 45(2)(c). These amendments permit the use of protected information in the circumstances set out in new section 65B of the Act, which permits the use of information obtained under a control order warrant issued on the basis of an interim control order, where the control order is subsequently declared void, in exceptionally limited circumstances.

792. Item 28 inserts a reference at the end of subsection 45(3) to 'or section 65B'. Subsection 45(3) of the Act provides that, subject to exceptions in subsections 45(4) and (5), protected information may not be admitted in evidence in any proceedings. Subsection 45(5) of the Act provides for a set of circumstances for which protected information may be lawfully used, communicated, published or admitted in evidence.

793. Item 29 inserts two additional paragraphs, 45(5)(j) and (k), which provide two sets of exceptions to the prohibition of the use of protected information in relation to control order warrants (j) or tracking device authorisations (k).

794. Paragraph 45(5)(j) will allow information to be obtained under a control order warrant, or relating to a control order warrant, or likely to enable the identification of a person, object or premises specified in a control order warrant, to be used, recorded, communicated, published or admitted into evidence to determine whether the control order is being complied with.

795. Paragraph 45(5)(k) will allow information obtained under a tracking device authorisation, or relating to a tracking device authorisation, or likely to enable the identification of a person, object or premises specified in a tracking device authorisation to be used, recorded, communicated, published or admitted into evidence to determine whether the control order is being complied with.

796. Subsection 45(6) prevents the use, recording, communication, or publication of information despite the exceptions provided for under paragraphs 45(4)(f) and 45(5)(a), (b) and (c), if that information is protected information that falls under subsection 44(d). Item 30 further applies this approach to the newly introduced paragraphs 45(5)(j) and (k).

797. Item 31 amends subsection 45(9) to enable protected information to be used in proceedings arising under, or relating to a matter arising under, a 'preventative detention order law'. It is intended to include application proceedings and any other proceedings, such as an appeal against such an order, a civil suit relating to such an order, or a prosecution relating to such an order.

**Item 32 – After section 46**

798. Item 32 inserts a new section 46A which deals with the destruction of records or reports comprised of information obtained under a control order warrant issued, or a tracking device authorisation given, to determine whether the control order, or any succeeding control order, has been, or is being, complied with prior to the control order having been served.

799. Section 46A requires information obtained prior to the control order having been served on the person—that is, prior to the person having been able to comply with the control order— to be destroyed as soon as practicable. However, the destruction requirement does not apply to records or reports that are likely to protect the public from a terrorist act, prevent a person engaging in, providing support for or facilitating a terrorist act or prevent hostile activity in a foreign country. Paragraph 46A(1)(f) reflects the overwhelming public interest in law enforcement agencies being permitted to use information in their possession to prevent acts of terrorism and hostile activity in foreign countries.

800. Paragraph 46A(2) displaces the operation of new section 6C in relation to new subsection 46A(1), which would otherwise deem a control order to be in force from the moment it is made.

**Items 33 and 34– Subsection 49(2)**

801. Section 49 sets out reporting and record-keeping requirements for surveillance device warrants, and emergency and tracking device authorisations. Subsection 49(1) requires chief officers of law enforcement agencies to report to the Minister in relation to each such warrant and authorisation issued or given to his or her agency. Subsections 49(2) and (3) set out the requirements for what must be contained in the report to the Minister as required under subsection 49(1).

802. Item 33 is a consequential amendment and inserts an additional subparagraph 49(2)(b)(xb) which requires the chief officer to report, in relation to each control order warrant, the details specified in subsection 49(2A).

803. Item 34 inserts new subsection 49(2A) that requires the report to give details of the benefit of the use of a surveillance device, and details of the general use made or to be made of any evidence or information stemming from the use of the surveillance device in:

- protecting the public from a terrorist act; or
- preventing the provision of support for, or the facilitation of, a terrorist act; or
- preventing the provision of support for, or the facilitation of, the engagement in a hostile act in a foreign country; or
- determining whether a control order has been, or is being, complied with.

804. This will ensure that law enforcement agencies are required to document and report the value of the use of surveillance devices used in relation to a control order.

**Item 35 – After section 49**

805. The Committee in its advisory report recommended (at Recommendation 11) that the Bill be amended to require the AFP to notify the Commonwealth Ombudsman of the issuing of a control order warrant and of any breaches of the requirements of the control order warrant regime.

806. The Bill goes beyond the recommendation of the Committee, and imposes consistent notification obligations on all law enforcement agencies, on the basis that if an agency has the ability to obtain a control order warrant, then the agency should be subject to the same oversight and accountability requirements as the AFP. For this reason, each law enforcement agency must adhere to the notification requirements in new section 49A.

807. New subsection 49A(4) also extends the notification obligations to apply in relation to tracking device authorisations given on the basis of a control order.

**Items 36 and 37 – At the end of section 50 and after section 50**

808. Items 36 and 37 set out circumstances in which the Minister must defer reporting on specific control order warrants until a subsequent annual report.

809. Item 37 inserts a new section 50A, which requires the public reporting of surveillance device warrants relating to a person subject to a control order to be deferred until a subsequent report in limited circumstances. Under subsection 50A, the chief officer of a Commonwealth agency or the chief officer of an eligible authority of a State must advise the Minister not to include the information in the Minister's report, which is tabled in Parliament, if the chief officer is satisfied that the information is 'control order information' as defined in new subsection 50A(6). This 'control order information' is information that, if made public, could reasonably be expected to enable a reasonable person to conclude that a control order warrant is likely to be, or is not likely to be, in force in relation to a particular premises, object or person.

810. Pursuant to subsection 50A(3) the Minister can act on the advice of the chief officer of the agency and not include the information in the report. If this is the case, there remains a positive obligation on the chief officer of the agency to advise the Minister to include the information in the next report if the chief officer is satisfied that a reasonable person could no longer draw those inferences from the information.

811. The reason for this new section is that control orders have historically been sought and made only rarely, with the effect that it is uncommon for there to be more than a limited number of control orders in force at any given time. If agencies were required to contemporaneously report on the number of warrants issued with respect to persons subject to control orders, and only a limited number of persons are subject to control orders at that time, annual reporting may effectively reveal that a particular person who is subject a control order is or is not also subject to covert surveillance.

812. The ability of a person to determine, or to speculate with a degree of certainty, whether they are, or are not, likely subject to surveillance may be further enhanced if the relevant control order contains particular conditions or restrictions that are particularly amenable to monitoring by way of a surveillance device. This would undermine the purpose and effectiveness of such warrants, by enabling and incentivising persons to either adopt counter-measures to avoid or reduce the effectiveness of covert surveillance (if the person determines they are, or are likely to be, under surveillance), or to breach the terms of the control order, or engage in terrorism or foreign hostilities-related activity (if the person determines they are not, or are unlikely to be, under surveillance).

**Item 38 – At the end of section 51**

813. Item 38 establishes a record-keeping obligation on agencies to keep advice given by the chief officer to defer the publication of control order information. In addition, new paragraph (m) requires agencies to retain the decision of the Minister on whether to include the information in the report.

**Item 39 – At the end of paragraph 52(1)(j)**

814. Section 52 lists records that the chief officer of a law enforcement agency is required to ensure are kept. Item 39 inserts a reference to the new subsection 46A(1). This will require that records be kept of the destruction of records pertaining to information obtained before a control order came into force.

**Item 40 – At the end of subsection 52(1)**

815. Pursuant to new subsection 50A(4), the chief officer of an agency must reconsider previous advice to defer the publication of control order information to determine whether the information should be included in the next Ministerial report. This item creates a record-keeping obligation in relation to that reconsideration by the chief officer where in the opinion of the chief officer the information remains 'control order information' for the purposes of section 50A.

**Item 41 – After subparagraph 53(2)(c)(iiib)**

816. Section 53 of the Act requires the chief officer of a law enforcement agency to cause a register of warrants and emergency and tracking device authorisations sought by law

enforcement officers of their agency to be kept. Subsection 53(2) of the Act specifies what must be included in the register in relation to surveillance device warrants.

817. Item 41 inserts a new subparagraph 53(2)(c)(iiic) to the Act to require that, in relation to control order warrants, the register must detail the date the control order was made. This is of particular importance as it will provide an overview in relation to control order warrants and authorisations for the Commonwealth Ombudsman, who is empowered under section 55 to oversee compliance with the Act.

**Item 42 – After subsection 55(2)**

818. This item is in response to Recommendation 11 of the Committee advisory report, which recommended that the Ombudsman report to the Attorney-General annually regarding the AFP's compliance with the requirements of the control order warrant regime.

819. Item 42 goes beyond the recommendation by the Committee, by empowering the Ombudsman to inspect a law enforcement agency's records (including all Commonwealth, state and territory agencies' records), to determine the extent of their compliance with the provisions mentioned in new subsection 49A(2), if the Ombudsman has received notification from a chief officer of a law enforcement agency that an officer has contravened a provision in new subsection 49A(2) and the contravention occurred in that period.

**Item 43 – At the end of section 61**

820. Item 43 inserts new subsections 61(4), (5) and (6) to allow the Minister to defer the inclusion of 'control order information' (see item 1) in the copy of the report he or she receives from the Commonwealth Ombudsman that is tabled in Parliament (but not from the copy that is provided to the relevant state or territory Minister with responsibility for the surveillance devices laws of that state or territory).

821. The reason for these new subsections is that control orders have historically been sought and made only rarely with the effect that it is uncommon for there to be more than a limited number of control orders in force at any given time. In such circumstances, the contemporaneous public reporting on agencies' compliance with the control order warrant regime may effectively reveal that a particular person who is subject a control order is or is not also subject to covert surveillance.

822. The ability of a person to determine, or to speculate with a degree of certainty, whether they are, or are not, likely subject to surveillance may be further enhanced if the relevant control order contains particular conditions or restrictions that are particularly amenable to monitoring by way of a surveillance device. This would undermine the purpose and effectiveness of such warrants, by enabling and incentivising persons to either adopt counter-measures to avoid or reduce the effectiveness of covert surveillance (if the person determines they are, or are likely to be, under surveillance), or to breach the terms of the control order or engage in terrorism or foreign hostilities-related activity (if the person determines they are not, or are unlikely to be, under surveillance).

823. As with the deferred reporting arrangements under new section 50A of the Act, and under the TIA Act, if the Minister defers publicly reporting on control order information, the Minister is required to reconsider including that information in each subsequent report.

**Item 44 – At the end of Division 3 of Part 6**

824. Item 44 inserts section 61A, which applies to the situation in which the chief officer of an agency has notified the Ombudsman that an officer has contravened a certain requirement (in subsection 49A(2)) and the Ombudsman decides not to conduct an inspection as a result. Such contraventions may be minor in nature, or may be similar in nature to other contraventions in relation to which the Ombudsman has conducted an inspection.

825. New section 61A permits the Ombudsman to include information on such contraventions in his or her report to the Minister under section 61, ensuring that the Minister, relevant state or territory Minister, Parliament and public have visibility of all contraventions of the control order warrant framework, including those where the Ombudsman has not conducted a specific inspection.

**Item 45 – After section 65**

826. New subsection 65A provides that a person is immune from being criminally liable for anything done, or omitted to be done, in good faith before the control order was declared void in the purported execution of a control order warrant, tracking device authorisation or use of a surveillance device without a warrant, or the purported exercise of a power or performance of a function or duty that is consequential on the warrant, authorisation or use.

827. This qualified immunity from criminal prosecution recognises the inherent risks assumed by law enforcement officers and persons assisting them in relying in good faith on legal authorities that may subsequently be declared void *ab initio*. Importantly, this qualified immunity does not:

- protect persons from criminal liability for acts done, or omitted to be done, otherwise than in good faith
- protect persons from criminal liability for acts done, or omitted to be done, subsequent to a control order being declared void (if, at the time, the person knew, or ought reasonably to have known, of the declaration), or
- protect law enforcement agencies from civil liability in these circumstances.

828. New section 65B permits the use of information obtained under a control order warrant. The intention of section 65B is that, despite a control order being declared void (which would therefore also invalidate the control order warrant *ab initio*), obtained information can be used to prevent or reduce the risk of a terrorist attack, serious harm to a person, or serious damage to property, or to apply for a PDO under respective Commonwealth, state and territory laws.

829. The provision is intended to address the unlikely scenario where:

- an interim control order has been issued in respect of a person;
- a law enforcement agency has duly obtained a control order warrant in relation to that person;
- under that control order warrant, the agency has obtained information that indicates that the person is likely to engage in a terrorist act, cause serious harm to a person, or cause serious damage to property;

- before the agency can act on that information, the interim control order is considered by a court at a confirmation hearing and declared void *ab initio* pursuant to subsection 104.14(6) of the *Criminal Code* on the grounds that, at the time of making the interim control order, there were no grounds on which to make the order.

830. As the existence of a valid control order is a condition for the issuing of a control order warrant, the likely effect of a court declaring an interim control order void *ab initio* pursuant to subsection 104.14(6) of the *Criminal Code* would be that any control order warrants predicated on that control order would also likely be void *ab initio*.

831. It is a fundamental principle of the Australian legal system that courts have a discretion as to whether or not information may be admitted as evidence into proceedings, irrespective of the manner in which the information was obtained. As an example, the *Bunning v Cross*[14] discretion places the onus on the accused to prove misconduct in obtaining certain evidence and to justify the exclusion of the evidence. This principle is expanded on in Commonwealth statute[15], where there is an onus on the party seeking admission of certain evidence to satisfy the court that the desirability of admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. This fundamental principle reflects the need to balance the public interest in the full availability of relevant information in the administration of justice against competing public interests, and demonstrates the role the court plays in determining admissibility of evidence.

832. However, the SD Act departs from these fundamental principles, by imposing strict prohibitions on when material under those Acts may be used, communicated or admitted into evidence.[16] Under the SD Act, it is a criminal offence for a person to deal in information obtained under the Act for any purpose, unless the dealing is expressly permitted under one or more of the enumerated and exhaustive exceptions to the general prohibition. This prohibition expressly overrides the discretion of the judiciary, both at common law and under the Evidence Act, to admit information into evidence where the public interest in admitting the evidence outweighs the undesirability of admitting it, given the manner in which it was obtained. There is also a risk that the prohibition might be interpreted, either by a court considering the matter after-the-fact, or by an agency considering the question *in extremis*, to override the general defence to criminal responsibility under the *Criminal Code*.

833. For this reason, the Bill will insert new section 65B to the SD Act which will expressly permit agencies to rely on such information to prevent, or lessen the risk, of a terrorist act, serious harm to a person, or serious damage to property. This provision will also permit such information to be used to apply for, and in connection with, a PDO.

---

[14] (1978) 141 CLR 54.
[15] Section 138 of the *Evidence Act 1995 (Cth)*.
[16] See section 45 of the SD Act.

## Schedule 11—Offence of advocating genocide

### *Criminal Code Act 1995*

### Overview

835. Division 80 of the *Criminal Code* currently contains a range of offences for urging or advocating certain conduct, including terrorism, which attracts a penalty of seven years imprisonment.

836. The amendments in this Schedule create a new offence of advocating genocide. The offence applies to advocacy of genocide of people who are outside Australia or the genocide of national, ethnic, racial or religious groups within Australia.

### Item 1 – Part 5.1 of the *Criminal Code* (heading)

837. This item replaces the existing heading with a new heading 'Part 5.1—Treason, urging violence and advocating terrorism or genocide', acknowledging the inclusion of a new offence for advocating genocide in Part 5.1.

### Item 2 – Division 80 of the *Criminal Code* (heading)

838. This item replaces the existing heading with a new heading 'Division 80—Treason, urging violence and advocating terrorism or genocide', acknowledging the inclusion of a new offence for advocating genocide in Division 80.

### Item 3 – Subdivision C of Division 80 of the *Criminal Code* (heading)

839. This item replaces the existing heading with a new heading 'Subdivision C—Urging violence and advocating terrorism or genocide', acknowledging the inclusion of a new offence for advocating genocide in Subdivision C of Division 80.

### Item 4 – At the end of Subdivision C of Division 80 of the *Criminal Code*

840. This item inserts new section 80.2D providing the new 'Advocating genocide' offence at the end of Subdivision C of Division 80.

841. New subsection 80.2D(1) creates a new offence of advocating genocide.

842. A person will commit an offence if the person advocates genocide, and the person advocates genocide reckless as to whether another person will engage in genocide.

843. The new offence does not include a requirement of 'publicly' advocating genocide, which is consistent with Recommendation 18 of the Committee advisory report. The Committee noted submissions highlighting that, depending on the context, private advocacy of genocide might be more dangerous than public advocacy and, further, defining 'publicly' for the purposes of the offence could prove difficult. The Committee recommended removing the term 'publicly' from the offence, as drafted for the 2015 Bill, so that it would be consistent with the existing 'advocating terrorism' offence in the *Criminal Code*, for which no such limitation applies.

844. The inclusion that a person advocates genocide reckless as to whether another person will engage in genocide is also consistent with Recommendation 17 of the Committee advisory report.

845. Accordingly, a successful prosecution will require evidence that the person intentionally communicated something in circumstances where there was a substantial risk that another person would take that speech as advocating the commission of a genocide offence.

846. Where there is sufficient evidence, the existing offences of incitement (section 11.4 of the *Criminal Code*) or urging violence (in Division 80 of the *Criminal Code*) will continue to be pursued. These offences require proof that the person intended the crime or violence to be committed, and there are circumstances where there is insufficient evidence to meet that threshold. Groups or individuals advocating genocide can be very deliberate about the precise language they use, even though their overall message still has the impact of encouraging others to engage in genocide.

847. Furthermore, in the current threat environment, the use of social media by hate preachers means the speed at which persons can become radicalised and could prepare to carry out genocide may be accelerated. It is no longer the case that explicit statements (which would provide evidence to meet the threshold of intention and could be used in a prosecution for inciting genocide) are required to inspire others to take potentially devastating action against groups of individuals. This new offence is directed at those who supply the motivation and imprimatur, particularly where a person advocating genocide holds significant influence over other people who sympathise with, and are prepared to fight for, the genocide of a race or other group of individuals.

848. Law enforcement agencies require tools to intervene earlier in the radicalisation process to prevent and disrupt the radicalisation process and engagement in terrorist activity. This new offence would supplement existing offences, such as those in Division 80 of the *Criminal Code*, that prohibit urging violence and advocating terrorism, and is intended to be one of those tools.

849. New subsection 80.2D(1) includes a note that refers readers to the existing defence in section 80.3 of the *Criminal Code* for acts done in good faith. This defence protects the implied freedom of political communication, and specifically excludes from the offence, among other things, publishing a report or commentary about a matter of public interest in good faith.

850. The offence carries a maximum penalty of seven years imprisonment, recognising the severity of the potential consequences of encouraging others to engage in genocide offences.

851. New subsection 80.2D(2) 'double jeopardy' provides that a person cannot be tried in an Australian court for the offence of advocating genocide if the person has already been convicted or acquitted by the International Criminal Court in relation to that conduct.

852. New subsection 80.2D(3) (Definitions) provides that, for the purposes of the offence in subsection 80.2D(1), 'advocate' means counsel, promote, encourage or urge the commission of a genocide offence. Those expressions will have their ordinary meaning. The terms 'promote' and 'encourage' are not defined. The ordinary meaning of each of the relevant expressions varies, but it is important that they be interpreted broadly to ensure a

person who advocates genocide does not escape punishment by relying on a narrow construction of the terms or one of the terms. However, some examples of the ordinary meaning of each of the expressions follow: to 'counsel' the doing of an act (when used as a verb) is to urge the doing or adoption of the action or to recommend doing the action; to 'encourage' means to inspire or stimulate by assistance or approval; to 'promote' means to advance, further or launch; and 'urge' covers pressing by persuasion or recommendation, insisting on, pushing along and exerting a driving or impelling force.

853. While there may be some overlap between the expressions, it is clear that they do not cover merely commenting on or drawing attention to a factual scenario, particularly when combined with relevant defences. For example, conduct such as pointing out in good faith that a government policy is mistaken, contains an error, or is defective, is clearly covered by the defence in paragraphs 80.3(1)(a) and (b) of the *Criminal Code*. Similarly, conduct such as publishing a report or commentary about a matter of public interest in good faith is covered by the defence in paragraph 80.3(3). This will not stifle true debate that occurs—and should occur—within a democratic and free society. The new offence is designed to capture those communications that create an unacceptable risk of the commission of genocide. Accordingly, a successful prosecution will require evidence that the person intentionally communicated something in circumstances where there is a substantial risk that someone would take that speech as advocating the commission of a genocide offence, or where a person was reckless as to whether another person will engage in genocide, as a result of their conduct.

854. New subsection 80.2D(3) defines 'genocide' to mean an offence contrary to Subdivision B of Division 268 of the *Criminal Code* (section 268.3 (genocide by killing), section 268.4 (genocide by causing serious bodily harm), section 268.5 (genocide by deliberately inflicting conditions of life calculated to bring about physical destruction), section 268.6 (genocide by imposing measures intended to prevent births), or section 268.7 (genocide by forcibly transferring children)). Further, for the purposes of new subsection 80.2D(2), a genocide offence does not include an offence against section 11.1 (attempt), section 11.4 (incitement) or section 11.5 (conspiracy) to the extent that it relates to a terrorism offence; and does not include a terrorism offence that a person is taken to have committed because of section 11.2 (complicity and common purpose), section 11.2A (joint commission) or section 11.3 (commission by proxy).

855. Whether specific conduct, such as making or commenting on a particular post on the internet or the expression of support for committing genocide, is captured by the offence will depend on all the facts and circumstances. Whether a person has actually 'advocated' the commission of a genocide offence will ultimately be a consideration for judicial authority based on all the facts and circumstances of the case.

856. New subsection 80.2D(4) makes it clear that a reference to advocating genocide includes a reference to advocating genocide, even if:

- genocide does not occur
- it is in relation to a specific genocide offence, or
- it is in relation to more than one genocide offence.

**Schedule 12**

***Australian Security Intelligence Organisation Act 1979***

**Part 1—Main amendments**

**Overview**

857. This Schedule amends section 40 of the ASIO Act to enable ASIO to furnish security assessments directly to a state or territory or an authority of a state or territory.

858. Under current arrangements, ASIO can only furnish a security assessment either directly to a state or territory in respect of a designated special event or in all other cases indirectly via a Commonwealth agency. Such arrangements are resource intensive and significantly hinder the timely provision of security assessments to state and territory authorities.

859. Enabling ASIO to furnish security assessments directly to a state or territory or an authority of a state or territory will enhance the timely provision of security information to those authorities. It is not intended that the accountability mechanisms already provided for in the ASIO Act in relation to rights of notice and review will be altered by the proposed amendment; nor the range of prescribed administrative actions by states or territories which can be the subject of security assessments. In order to implement Recommendation 19 of the Committee advisory report, the Bill also amends section 61 of the ASIO Act to ensure that states and state authorities will be required to treat findings of the AAT, to the extent that they do not confirm a security assessment, as superseding that assessment.

**Technical and consequential amendments (items 1, 2, 3 and 7)**

860. To give full effect to amendments to section 40, subsections 35(1), 38(3), 38(6) and paragraph 65(1)(b) will be amended to include 'State or authority of a State' into the existing provisions, to ensure their application to State agencies in addition to their current application to Commonwealth agencies.

861. 'State' as defined in section 4 of the ASIO Act includes the Australian Capital Territory and the Northern Territory.

862. For example, item 1 will amend the definition of 'security assessment' in section 35(1) which previously defined a security assessment to include (among other criteria) a statement in writing furnished by ASIO to a Commonwealth agency to also include a statement in writing furnished to a 'State or authority of a State'.

**Item 4 – Subsection 40(1)**

863. This item repeals and replaces existing subsection 40(1) and paragraphs 40(1)(a) and 40(1)(b).

864. Item 4 gives effect to the policy intention of amending section 40, to enable ASIO to furnish security assessments directly to states and territories or an authority of a state or territory. This policy is consistent with the definition of the term 'security' in section 4 of the ASIO Act which relates to both the States and the Commonwealth.

865. New subsection 40(1) removes the requirement in existing subsection 40(1) that prescribed administrative action in respect of a person by a State or an authority of a State 'would affect security in connection with matters within the functions and responsibilities of a Commonwealth agency'.

866. New paragraph 40(1)(a) provides for ASIO to furnish a security assessment to a Commonwealth agency for transmission to a state or an authority of a state for use in considering the taking of prescribed administrative action. This amendment ensures that ASIO could still furnish a security assessment to a Commonwealth agency to transmit to a state in circumstances where it is appropriate to do so (for example an event where security is an issue relevant to both the Commonwealth and states such as a significant political or sporting event that requires coordination at a Commonwealth level).

867. New paragraph 40(1)(b) provides for ASIO to furnish a security assessment to a State or an authority of a State for use in considering the taking of a prescribed administrative action. Currently, under paragraph 40(1)(b) ASIO can only furnish a security assessment directly to a state or territory if the prescribed administrative action would affect security in connection with a 'special event' (being an event designated as such by the Minister). Events that had been envisaged as a 'special event' under the current paragraph 40(1)(b) included major international intergovernmental meetings and major sporting events like the Olympics or Commonwealth Games (the relevant provision having first been added in the context of the Sydney Olympics). This amendment ensures that there no longer needs to be a connection with a special event in order for ASIO to furnish security assessments directly to a state or territory.

**Item 5 – Paragraph 40(2)(a)**

868. Currently, paragraph 40(2)(a) prevents ASIO from communicating directly to a state or an authority of a state either in the form of an assessment or otherwise any information, recommendation, opinion or advice concerning a person which ASIO knows is intended or likely to be used by the State or an authority of the State in considering prescribed administrative action in relation to that person.

869. Consistent with item 4, item 5 will amend paragraph 40(2)(a) to allow ASIO to pass such information directly to a State if it is in the form of an assessment. Paragraph 40(2)(a) will continue to prohibit ASIO from furnishing information, recommendations, opinions or advice, which ASIO knows is intended or likely to be used by a state in considering prescribed administrative action in relation to a person, that is not in the form of an assessment. A person's rights of notice and review in relation to an ASIO security assessment will not be altered.

**Item 6 – Subsection 40(3)**

870. This item repeals subsection 40(3) which required the Minister to notify the Director-General of an event designated as a special event. This amendment is a consequential amendment to paragraph 40(1)(b).

**Item 7 – Section 61**

871. Section 61 currently provides that a Commonwealth agency must treat any findings of the AAT, to the extent that they do not confirm an adverse or qualified security assessment,

as superseding that assessment. This item amends section 61 to ensure that a state or state authority must also treat inconsistent AAT findings as superseding a security assessment.

872. This amendment is not intended to interfere with a State or State authority's exercise of powers. A security assessment provided by ASIO is an 'assessment' of a given situation, defined in section 35 of the ASIO Act to include a recommendation, opinion or advice. Beyond the obligation in subsection 38(1) of the ASIO Act to give notice of the assessment to the subject, the Commonwealth does not require the State to respond in a particular way to the recommendation, opinion or advice.

873. This amendment represents a requirement for recipients of ASIO security assessments, and those who review or consider appeals from decisions to which the assessments are applied, to regard the AAT findings as supplanting the original assessment from the effective date of the findings. It remains entirely a matter for each State or State authority to determine the use to which an assessment is put.

**Item 8 – Subsection 65(1)(b)**

874. This item inserts 'State or authority of a State' to ensure that section 65 applies to state agencies in addition to Commonwealth agencies.

**Item 9 – Application of amendment of paragraph 65(1)(b)**

875. This item provides that the amendment of paragraph 65(1)(b) of the ASIO Act applies in relation to security assessments and communications furnished, or allegedly furnished, after the commencement of this Schedule.

**Part 2—Consequential amendments**

***Administrative Appeals Tribunal Act 1975***

**Technical amendments (items 10-14)**

876. The amendments to section 40 of the ASIO Act will require consequential amendments to sections 29B, 39A(2), (6), (7), (8) and (12), 39A(15)(b), 39A(15) and 43AAA(4) and 5 of the AAT Act to reflect the involvement that state and territory agencies may have in the AAT review of security assessments (as opposed to just a Commonwealth agency). Items 10-14 will insert either 'State or authority of a State' or 'State or authority' in the existing provisions to ensure their application to state agencies in addition to Commonwealth agencies.

877. For example, item 10 will amend section 29B by inserting 'State or authority of a State' so that following an application made to the AAT for the review of a security assessment, the AAT must cause a copy of the application to be given to the Director-General of Security and to the Commonwealth agency, 'State or authority of a State' to which the assessment was given.

**Schedule 13—Classification of publications etc.**

***Classification (Publications, Films and Computer Games) Act 1995***

**Item 1 – Paragraph 9A(2)(a)**

878. This item amends existing paragraph 9A(2)(a) of the Classification Act to align the definition of 'advocates' in the Classification Act with the updated definition as currently found in the *Criminal Code*.

879. Currently, subsection 9A(1) of the Classification Act provides that a publication, film or computer game that 'advocates' the doing of a terrorist act must be classified Refused Classification (or RC). Paragraph 9A(2)(a) of the Classification Act provides that for the purposes of section 9A (Refused Classification for publications, films or computer games that advocate terrorist acts) a publication, film or computer game 'advocates' the doing of a terrorist act if it directly or indirectly 'counsels' or 'urges' the doing of a terrorist act.

880. Historically, paragraph 9A(2)(a) of the Classification Act was adapted directly from paragraph 102.1(1A)(a) of the *Criminal Code* as it stood in 2007. The Explanatory Memorandum to the amending Act, the *Classification (Publications, Films and Computer Games) Amendment (Terrorist Material) Act 2007*, notes that the definition of 'advocates' should have the same meaning in the Classification Act when applied to a publication, film or computer game, as in the *Criminal Code* when applied to a terrorist organisation.

881. On 1 December 2014, the definition of 'advocates' in paragraph 102.1(1A)(a) of the *Criminal Code* was amended by the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014* (the Foreign Fighters Act), to ensure that in addition to 'counselling' or 'urging', an organisation 'advocates' the doing of a terrorist act if it 'promotes' or 'encourages' the doing of a terrorist act. However, the definition of 'advocates' in the Classification Act was not updated by the Foreign Fighters Act.

882. The Revised Explanatory Memorandum to the Foreign Fighters Act explains that the terms 'promotes' and 'encourages' are not defined. The ordinary meaning of 'promotes' the doing of a terrorist act could include conduct or statements such as launching a campaign to commit terrorist acts, and that the ordinary meaning of 'encourages' the doing of a terrorist act could include conduct or statements that inspire an individual to commit a terrorist act.

883. While there may be some overlap with the terms 'counsels' or 'urges' the doing of a terrorist act, which may include conduct such as inducement, persuasion or insistence, or to give advice about the doing of a terrorist act, the inclusion of the additional terms is designed to ensure coverage of a broader range of conduct that may be considered as advocating the doing of a terrorist act, beyond the existing conduct of 'counsels' or 'urges'.

884. The Committee advisory report supported the proposed amendment, noting that it considers it reasonable that publications, films and computer games should be refused classification on the basis of the same definition of advocacy of terrorism as that in the *Criminal Code*.

**Item 2 – Application**

885. This item provides that the amendment of the Classification Act in Item 1 applies in relation to the making of classifications on and after the commencement of this Schedule whether the classifications were applied for before, on or after that commencement.

## Schedule 14—Delayed notification search warrants

*Crimes Act 1914*

### Part 1—Amendments

886. The purpose of these amendments is to clarify the threshold requirements for the issue of a delayed notification search warrant (DNSW). The amendments clarify that, while an eligible officer applying for a DNSW must actually hold the relevant suspicions and belief set out in section 3ZZBA, the chief officer and eligible issuing officer need only be satisfied that there are reasonable grounds for the eligible officer to hold the relevant suspicions and belief.

887. These amendments do not make any substantive change to the requirements for obtaining a DNSW. The existing regime in Part IAAA already provides that an eligible officer may be required to swear or affirm the grounds for holding the relevant suspicions and belief. The amendments are intended to clarify that neither a chief officer nor an eligible issuing officer are required to personally suspect or believe the matters set out in section 3ZZBA. This is because the chief officer and eligible issuing officer are unlikely to be directly involved in the investigation giving rise to the need for a DNSW and are not in a position to personally suspect or believe the relevant matters.

**Item 1 – Section 3ZZAC (definition of *conditions for issue*)**

888. Item 1 repeals the definition of 'conditions for issue' in section 3ZZAC. This amendment is consequential to a range of other amendments to the DNSW regime.

**Item 2 – Section 3ZZBA**

889. This item repeals existing section 3ZZBA, removing the 'conditions for issue' in relation to the issue of a DNSW, and substitutes amended wording for the test that applies to when an eligible officer may seek authorisation from a chief officer to apply for a DNSW.

890. Currently, the request for a delayed notification search warrant requires reasonable grounds for suspecting and believing certain things. The regime could be interpreted as requiring the eligible officer who applies for the warrant, the chief officer who considers whether to authorise the application, and the eligible issuing officer who considers whether to issue the warrant to hold the relevant suspicions and belief—currently referred to as the 'conditions for issue'.

891. This amendment removes reference to 'conditions for issue' and substitutes new wording of the test for when an eligible officer may seek the chief officer's authorisation to apply for a DNSW.

892. Revised section 3ZZBA requires the eligible officer to personally suspect, and have reasonable grounds for suspecting, that:

- one or more eligible offences have been, are being, are about to be or are likely to be committed, and
- entry and search of particular premises will substantially assist in the prevention or investigation of one or more of those offences.

893. It also requires the eligible officer to believe, and have reasonable grounds for believing, that it is necessary for the entry and search of the premises to be conducted without the knowledge of the occupier of the premises or any other person present at the premises.

894. This amendment does not change the threshold of suspicion or belief that an eligible officer must have in order to seek authorisation to apply for a DNSW. Rather, the purpose of the amendment is to make clear that the eligible officer is required to personally hold the suspicions and belief referred to in the section.

**Item 3 – Subsections 3ZZBB(1) and (2)**

895. This item repeals subsections 3ZZBB(1) and (2) and inserts new subsections 3ZZBB(1A), (1) and (2). These subsections provide the test that applies when a chief officer is considering whether to authorise an eligible officer to apply for a DNSW.

896. New subsection 3ZZBB(1A) provides that, where an eligible officer seeks the chief officer's authorisation to apply for a DNSW in relation to particular premises, the conditions in section 3ZZBB must be met.

897. New subsection 3ZZBB(1) provides that, before authorising an eligible officer to apply for a DNSW, the chief officer must be satisfied that there are reasonable grounds for the eligible officer to hold the suspicions and belief set out in section 3ZZBA. However, the chief officer does not need to personally suspect or believe those matters.

898. New subsection 3ZZBB(2) provides that the chief officer may authorise the application orally, provided there are reasonable grounds for the eligible officer to hold the relevant suspicions and belief, and either the matter is urgent, or delay in authorising the DNSW would frustrate the effectiveness of executing the warrant.

**Item 4 – Subsection 3ZZBC(1) (paragraph (a) of note 1)**

899. Item 4 amends note 1 to subsection 3ZZBC(1), which sets out the factors to be addressed in an application for a DNSW. The amendment removes the reference to 'conditions for issue' and provides that the application must address why there are reasonable grounds for:

- suspecting that one or more eligible offences have been, are being, are about to be or are likely to be committed
- suspecting that entry and search of the premises will substantially assist in the prevention or investigation of one or more of those offences, and
- believing that it is necessary for the entry and search of the premises to be conducted without the knowledge of the occupier of the premises or any other person present at the premises.

900. This is in order to provide an eligible issuing officer with enough information to be satisfied that there are reasonable grounds for the eligible officer to hold the relevant suspicions and belief.

**Item 5 – Paragraph 3ZZBD(1)(b)**

901. This item amends paragraph 3ZZBD(1)(b) by removing the reference to 'conditions for issue' and substitutes new requirements that must be met before an eligible issuing officer may issue a DNSW.

902. This amendment clarifies that the eligible issuing officer is not required to personally hold the relevant suspicions and belief before issuing a DNSW. Rather, the eligible issuing officer must be satisfied that there are reasonable grounds to support the eligible officer's suspicions and belief.

**Item 6 – Subsection 3ZZBD(1)**

903. This item amends subsection 3ZZBD(1) by replacing the reference to 'premises' at the end of subsection 3ZZBD(1) with a reference to the 'main premises'. This corrects a drafting error by clarifying that an eligible issuing officer can issue a DNSW in relation to particular or main premises following receipt of an application, and provided the eligible issuing officer is satisfied by information on oath or affirmation that there are reasonable grounds for the eligible officer to hold the relevant suspicions and belief.

**Item 7 – Paragraph 3ZZBD(2)(a)**

904. This item amends paragraph 3ZZBD(2)(a) by inserting the words 'or offences' after the word 'offence'. This is a technical amendment to ensure consistency with the requirement in paragraph 3ZZBA(a) that an eligible officer must hold a suspicion in relation to one or more eligible offences, and acknowledges that the warrant may relate to the investigation of more than one offence.

**Item 8 – At the end of paragraph 3ZZBD(2)(d)**

905. This item inserts the words 'or those offences' after the word 'offence'. This is a technical amendment to ensure consistency with the requirement in paragraph 3ZZBA(a) that an eligible officer must hold a suspicion in relation to one or more eligible offences, and acknowledges that the warrant may relate to the investigation of more than one offence.

**Item 9 – At the end of subparagraph 3ZZBD(2)(e)(ii)**

906. This item inserts the words 'or those offences' after the word 'offence'. This is a technical amendment to ensure consistency with the requirement in paragraph 3ZZBA(a) that an eligible officer must hold a suspicion in relation to one or more eligible offences, and acknowledges that the warrant may relate to the investigation of more than one offence.

**Item 10 – Paragraph 3ZZBE(1)(e)**

907. This item inserts the words 'or those offences' after the word 'offence'. This is a technical amendment to ensure consistency with the requirement in paragraph 3ZZBA(a) that an eligible officer must hold a suspicion in relation to one or more eligible offences, and acknowledges that the warrant may relate to the investigation of more than one offence.

**Item 11 – Paragraph 3ZZBF(5)(c)**

908. This item removes the reference to 'conditions for issue' in paragraph 3ZZBF(5)(c). The amendment provides that an eligible issuing officer may complete and sign a warrant if satisfied that there are reasonable grounds for the eligible officer's suspicions and belief referred to in section 3ZZBA.

909. This amendment clarifies that the eligible issuing officer is not required to personally hold a suspicion or belief before signing the delayed notification search warrant. However, the eligible issuing officer must be satisfied that there are reasonable grounds for the eligible officer to hold the relevant suspicions and belief.

**Item 12 – Subparagraph 3ZZFE(2)(c)(ii)**

910. This item inserts the words 'or offences' after the word 'offence'. This is a technical amendment to ensure consistency with the requirement in paragraph 3ZZBA(a) that an eligible officer must hold a suspicion in relation to one or more eligible offences, and acknowledges that the warrant may relate to the investigation of more than one offence.

**Part 2—Application of amendments**

**Item 13 – Application of amendments**

911. This item confirms that the present amendments have no effect on the validity of a DNSW issued, or an authorisation or application made, before these amendments commenced.

## Schedule 15—Protecting national security information in control order proceedings

### Part 1 – Main amendments

*National Security Information (Criminal and Civil Proceedings) Act 2004*

**Overview**

912. The objective of the NSI Act is to prevent the disclosure of information in federal criminal proceedings and civil proceedings where disclosure is likely to prejudice national security, except to the extent that preventing the disclosure would seriously interfere with the administration of justice. 'National security' means 'Australia's defence, security, international relations or law enforcement interests' (section 8).

913. The NSI Act provides a range of protections for sensitive information, the disclosure of which is likely to prejudice national security. These options include allowing sensitive information to be redacted, and preventing a witness from being required to give evidence.

914. In some circumstances, information will be so sensitive that existing protections under the NSI Act are insufficient. For example, critical information supporting a control order may reveal law enforcement or intelligence sources, technologies and methodologies associated with gathering and analysing information. The inadvertent or deliberate disclosure of such material may endanger the safety of individuals as well as the general public, or jeopardise sources and other intelligence methods. However, the inability to provide such information to a court may mean that a control order is unable to be obtained.

915. The speed of counter-terrorism investigations is increasing. In order for control orders to be effective, law enforcement need to be able to act quickly, and be able to present sensitive information (which is in the form of admissible evidence) to a court as part of a control order proceeding without risking the integrity, safety or security of the information or its source. However, it is equally important that the court is able to consider sensitive information without being constrained in its ability to control proceedings and ensure procedural fairness and the administration of justice.

916. This Schedule amends the NSI Act by enabling a court to make three new types of orders in control order proceedings under Division 104 of the *Criminal Code*. The effect of these court orders will be to allow an issuing court to consider information in control order proceedings (subject to the rules of evidence and other safeguards) which is not disclosed to the subject of the control order or their legal representative.

917. A control order proceeding under Division 104 of the *Criminal Code* is a civil proceeding for the purpose of the NSI Act.

**Procedural requirements for control orders**

918. Control orders require a detailed application to be prepared and presented to an issuing court.

919. Division 104 of the *Criminal Code* contains certain express statutory protections for the subject of the order. These include:

- Under section 104.5 an interim control order must set out a summary of the grounds on which the order is made, but does not need to include information that would likely prejudice national security. Given the order is made by the court, it is the court that determines what information the summary contains.
- If the AFP elects to confirm the interim control order, under section 104.12A the AFP must provide:
    - the statement of facts relating to why the order should or should not be made, and
    - the explanation as to why each of the proposed obligations, prohibitions or restrictions should be imposed on the person,

  that were used in the AFP's application for the interim control order, with the exception of material that the AFP may seek to protect for reasons of national security.
- Paragraph 104.12A(2)(a)(iii) also requires the AFP to serve personally on the person any other details required to enable the person to understand and respond to the substance of the facts, matters and circumstances which will form the basis of the confirmation of the control order.
- When a court hears a confirmed control order application, section 104.14 expressly preserves the rights of the subject of the order, such as the right to call witnesses and present material.

920. These statutory protections expressly preserve the procedural rights of the subject of the control order, and ensure they know the substance of the allegations that are made against them. They operate in addition to any other applicable procedural rights in federal civil proceedings, such as the normal processes of discovery, in which a party to a proceeding is entitled to obtain much of the material relied upon by the other party. Likewise, the AFP can seek to rely on traditional common law public interest immunity claims and provisions under the NSI Act to withhold certain information on national security grounds.

921. Section 104.14(2) expressly preserves the court's inherent power to control proceedings in relation to the confirmation of an interim control order. Any evidence adduced or submissions made by the AFP at a control order confirmation hearing is subject to the ordinary rules of evidence applicable to federal civil proceedings set out in the Evidence Act (section 104.28A(2)).

922. Accordingly, although there are existing references in Division 104 of the *Criminal Code* to national security redactions, there are no provisions in that Division which permit evidence to be used and considered by an issuing court in a control order confirmation (or variation) proceeding that the subject of the control order cannot access and contest. The NSI Act also does not permit this outcome.

**Invoking the NSI Act**

923. The NSI Act must be 'invoked' in a proceeding before the Act can apply to that proceeding. In a federal criminal proceeding, the prosecutor can invoke the NSI Act by giving notice in writing to the defendant, the defendant's legal representative and the court that the NSI Act applies to the proceeding. In a civil proceeding, the NSI Act is invoked by the Attorney-General giving notice in writing to the parties to the proceeding, the legal

representatives of the parties and the court that the Act applies to the proceeding. Unless and until this notice is given the NSI Act will not apply to the court proceeding. A control order proceeding under Division 104 of the *Criminal Code* is a civil proceeding for the purpose of the NSI Act.

**Existing orders for civil proceedings**

924. If the Attorney-General has invoked the NSI Act and issues a non-disclosure certificate under section 38F or a witness exclusion certificate under section 38H of the NSI Act, the court must hold a closed hearing in accordance with section 38I. The purpose of the closed hearing is for the limited purpose of addressing whether information potentially prejudicial to national security may be disclosed and if so, in what form, and whether to allow a witness to be called. For the purposes of this Schedule, the closed hearing under subsection 38G(1) or 38H(6) will be referred to as the NSI hearing. The court has the discretion to exclude non-security cleared parties, their non-security cleared legal representatives and non-security cleared court officials from the hearing where the court considers that disclosing the relevant information to these persons would likely prejudice national security.

925. Following the NSI hearing, the court must make one of four possible orders under section 38L. The court may order that:

- the information may be disclosed with appropriate deletions, redactions and summaries of information or facts (subsection 38L(2))
- the information must not be disclosed (subsection 38L(4))
- the information may be disclosed (subsection 38L(5)), or
- when determining whether to call a witness, that either the relevant party must not or may call the person as a witness (subsection 38(6)).

926. These orders do not permit evidence to be adduced in the substantive proceeding that has been withheld from the affected party or their legal representative. Accordingly, if the court orders that some or all of the information should not be disclosed to the respondent or their legal representative, that information cannot then be used in the substantive control order proceeding.

927. The NSI Act is designed to be flexible and ensure the court has the ability to conduct the proceeding in a manner it considers appropriate. The NSI Act does not prevent the court from making other protective orders such as upholding public interest immunity claims under common law, or making orders under other legislation.

**Proposed amendments—Revised section 38J**

928. This Schedule amends the NSI Act by enabling a court to make three new types of orders in control order proceedings under Division 104 of the *Criminal Code*. The three new orders provide that:

- the subject of the control order and their legal representative may be provided with a redacted or summarised form of the national security information. However, the court may consider all of the information contained in the original source document, even where that information has not been provided in the redacted or summarised form (new subsection 38J(2))

- the subject of the control order and their legal representative may not be provided with any information contained in the original source document. However, the court may consider all of that information (new subsection 38J(3)), or
- a witness may be called and the information provided by the witness need not be disclosed to the subject of the control order or their legal representative. However, the court may consider all of the information provided by the witness (new subsection 38J(4)).

929. The amendments provide that at the NSI hearing to review the Attorney-General's certificate in relation to a control order proceeding, the Attorney-General may request the court to make one of the three new orders under revised section 38J. The court has the discretion to make one of the orders, or make no orders at all, under section 38J. Where the court declines to make an order under revised section 38J, it must make one of the existing orders under section 38L.

**Features of the new orders**

*Applicability*

930. The new orders will only be available in control order proceedings under Division 104 of the *Criminal Code*.

*Presence at the NSI hearing*

931. The amendments provide that at the NSI hearing, the Attorney-General (or the Attorney-General's legal or other representative) may request the court to order that one or more specified parties to the control order proceeding and their legal representatives not be present during the NSI hearing. The discretion to make such an order rests with the court. Accordingly, even if the individual's legal representative is security cleared, the court may exclude them from the closed hearing to determine if or how information should be disclosed in the control order proceeding, if the court considers it appropriate.

932. However, the amendments contained in Part 2 of Schedule 15, relating to special advocates, will allow for the court to appoint a special advocate to be present during the NSI hearing where the subject of the control order (or the proposed control order) and their legal representative have been excluded, and in the substantive control order proceeding when information that is the subject of a revised section 38J order is considered by the court.

*Prerequisite for granting an order under revised section 38J*

933. In determining whether to make an order under revised section 38J, the court must be satisfied that the subject of the control order (or proposed control order) has been given sufficient information about the allegations on which the control order request was based to enable effective instructions to be given in relation to those allegations. This formulation adopts the minimum standard of disclosure that was recommended in the Committee advisory report.

934. Accordingly, the subject of the control order application must be given sufficient information about the allegations on which the control order application is sought (or varied) by the AFP. The precise amount of information necessary to discharge this standard will depend on the facts and circumstances of each case.

935. It is intended that the degree of information provided will enable the subject to effectively instruct a legal representative (or themselves, if they are self-represented).

936. For example, if a control order application alleged the subject had attended a terrorist training camp in a foreign country, the subject may only be informed of that allegation in general terms, if a court was satisfied disclosure of further and more detailed information about the person's attendance at that terrorist training camp would involve an unacceptable risk to sensitive national security intelligence sources.

*Factors the court must consider before making an order under revised section 38J*

937. In determining whether to make any of the three new orders under revised section 38J, the court must consider:

- the risk to prejudice to national security if an order were not made
- whether an order under revised section 38J would have a substantial adverse effect on the substantive hearing in the proceeding, and
- any other matter the court considers relevant.

938. Unlike orders under existing section 38L, there is no requirement in revised section 38J for the court to give the greatest weight to the need to protect national security.

**Item 1 – Subsection 19(4)**

939. Item 1 amends subsection 19(4) to provide that if a court considers a particular matter in making an order under revised section 38J, the court can still later stay the proceeding on a ground involving that same matter, including that the making of an order under revised section 38J would have a substantial adverse effect on the substantive hearing in the proceeding.

940. The purpose of this amendment is to confirm that the court has the power to stay control order proceedings where one of the new orders under revised 38J has been made. This amendment ensures that, for instance, even if the court considers the effect on the control order proceeding in deciding whether to make an order under revised section 38J, the court will not be prevented from later staying the control order proceeding on the ground that the order under revised section 38J would have a substantial adverse effect on the relevant person.

**Item 2 – Subparagraphs 38D(2)(a)(ii) and (b)(ii)**

941. Section 38D outlines the procedure for a party to a civil proceeding to notify the Attorney-General if the party knows or believes that national security information may be disclosed in the proceedings. The purpose of this provision is to trigger the Attorney-General's consideration of whether to issue a non-disclosure certificate or witness exclusion certificate under section 38F or section 38H. However, where the Attorney-General is aware of the potential disclosure under other mechanisms of the NSI Act, notice is not required to be given.

942. Item 2 amends subparagraphs 38D(2)(a)(ii) and (b)(ii) to provide that a party does not need to give the Attorney-General notice where the information to be disclosed is the subject

of one of the new orders in force under revised section 38J or where the disclosure of the information by the witness is the subject of an order under that section. This item extends the existing exception to the notice requirements set out in subsection 38D(1) for orders in force under sections 38B and 38L to revised section 38J.

**Item 3 – Subparagraphs 38E(2A)(c)(ii)**

943. Section 38E sets out the procedure for when a party to a civil proceeding knows or believes a witness will disclose national security information in answering a question whilst testifying in the proceeding.

944. Item 3 amends subparagraph 38E(2A)(c)(ii) to provide that a party or legal representative need not advise the court of that knowledge or belief where disclosure of the information is already the subject of an order in force under revised section 38J. This item extends the existing exception to the notice requirements for orders in force under sections 38B and 38L.

**Item 4 – Paragraph 38E(4)(b)**

945. If the court is advised that a witness' testimony will disclose national security information, the court must order that the witness give the court a written answer to the question. Subsection 38E(4) provides that once the court has received a written answer from the witness, the court must adjourn the proceedings to the extent necessary to ensure that the information is not disclosed and the Attorney-General can consider the information. Item 4 amends paragraph 38E(4)(b) to provide that the court need not adjourn proceedings under subsection 38E(4) where the information disclosed by the written answer is the subject of an order in force under revised section 38J. This item extends the existing exception for orders in force under sections 38B and 38L.

**Item 5 – Paragraph 38F(6)(b)**

946. Item 5 amends paragraph 38F(6)(b) to provide that a certificate of the Attorney-General will only lapse after the court has made an order under revised section 38J or section 38L and any appeals in relation to that order have ceased, unless the certificate is revoked by the Attorney-General.

**Item 6 – Paragraphs 38G(1)(a), (b) and (c)**

947. Section 38G outlines the process that applies if the Attorney-General has given a non-disclosure certificate under section 38F. Item 6 amends paragraphs 38G(1)(a), (b) and (c) to provide that if the Attorney-General gives a certificate under section 38F, the court must hold an NSI hearing at the times prescribed in those paragraphs to decide whether to make an order under revised section 38J (if the Attorney-General has requested the court to make an order under that section) or 38L in relation to the disclosure of the information.

**Item 7 – Subsection 38G(3)**

948. Item 7 amends subsection 38G(3) to provide that the closed hearing requirements under section 38I apply to a hearing to decide whether to make an order under revised section 38J (i.e. the NSI hearing).

**Item 8 – Paragraphs 38H(5)(b), (6)(a) and (6)(b)**

949. Item 8 amends paragraph 38H(5)(b) to provide that a witness exclusion certificate only ceases to have effect after the court has made an order under revised section 38J or section 38L and any appeals in relation to that order have ceased, unless the certificate is revoked by the Attorney-General before then.

950. Item 8 also amends paragraph 38H(6)(a) so that if the witness exclusion certificate is given to the court before the substantive control order proceeding begins, the court must hold an NSI hearing to decide whether to make an order under revised section 38J or section 38L in relation to the calling of the witness, before the proceeding begins.

951. Item 8 also amends paragraph 38H(6)(b) to provide that if the witness exclusion certificate is given to the court after the substantive control order proceeding begins, the court must adjourn the control order proceeding for the purpose of holding an NSI hearing to decide whether to make an order under revised section 38J or section 38L in relation to the calling of the witness.

**Item 9 – Subsection 38H(7)**

952. Item 9 amends subsection 38H(7) to provide that the closed hearing requirements under section 38I apply to a hearing to decide whether to make an order under revised section 38J (i.e. the NSI hearing).

**Item 10 – Before section 38I**

953. Item 10 inserts new Subdivision A (of Division 3) into Part 3A of the NSI Act. Subdivision A covers the closed hearing requirements under section 38I.

**Item 11 – Subsection 38I(1)**

954. Item 11 amends the closed hearing requirements to facilitate their use in control order proceedings under Division 104 of the *Criminal Code* if the court makes an order under new subsections 38J(2), (4) or (5).

955. The effect of this amendment is to ensure that the closed hearing requirements under section 38I apply in two separate circumstances. Firstly, the closed hearing requirements will apply, as they currently do, when the court is considering if or how national security information should be disclosed in a civil proceeding in accordance with subsections 38G(1) or 38(H) (i.e. the NSI hearing). Secondly, during a control order proceeding under Division 104 of the *Criminal Code*, the closed hearing requirements will apply when information is disclosed to the court that is the subject of an order under new subsections 38J(2), (4) or (5). This is also reflected in new paragraphs 38J(2)(d), 38J(3)(c) and 38J(4)(b) (see Item 21).

**Item 12 – Subsection 38I(1) (note)**

956. Item 12 modifies the note to subsection 38I(1) to make clear that although new subsections 38J(2), (3) and (4) provide for closed hearing requirements to apply to certain hearings, it does not prevent the court from exercising any powers that it otherwise possesses (for example, to exclude persons from other hearings or to prevent publication of evidence).

**Item 13 – After subsection 38I**

957. Item 13 inserts new subsection 38I(3A) which allows the court to order that one or more specified parties to the proceeding and their legal representative may be excluded from the NSI hearing. That hearing is the closed hearing pursuant to the requirements under section 38I that is held in order to determine if and how the information should be disclosed in the substantive proceeding. This order can only be made if the substantive proceeding is a control order proceeding under Division 104 of the *Criminal Code*.

958. New subsection 38I(3A) provides that the Attorney-General (or the legal or other representative of the Attorney-General) can request the court to make an order that one or more parties to the proceeding and their legal representatives should not be present at any part of the NSI hearing in which the Attorney-General (or the legal or other representative of the Attorney-General) gives detail of the information or gives information in arguing why the information should not be disclosed, or why the witness should not be called to give evidence, in the proceeding. Accordingly, the court may exclude the subject of the control order and their legal representative, even if they have an appropriate security clearance. The court has discretion as to whether to make an order under new subsection 38I(3A).

959. If an order under revised section 38J is made, a new subsection 38I(3A) order does not need to be sought by the Attorney-General in order to exclude the subject of the control order and their legal representative from the substantive control order proceeding when the information that is the subject of the revised section 38J order is considered by the court. Instead, as outlined in the note to new subsection 38I(3A), a revised section 38J order will provide for the automatic exclusion of the subject of the control order and their legal representative (see new paragraphs 38J(2)(e), 38J(3)(d) or 38J(4)(c)) from parts of the substantive control order proceeding when information that is the subject of the order is considered by the court.

**Item 14 – Paragraph 38I(5)(a)**

960. Item 14 amends paragraph 38I(5)(a) to provide that the existing requirement for the court to make and keep a record of the closed hearing, whether before or after it makes an order under section 38L, also applies to closed hearings where a court makes an order under revised section 38J.

**Item 15 – Subsection 38I(6)**

961. Item 15 corrects an error in subsection 38I(6) by removing a reference to section 38K which no longer exists in the NSI Act.

**Item 16 – Paragraph 38I(9)(a)**

962. Subsection 38I(9) requires the court to allow each party's legal representative with an appropriate security clearance (or a party who has been given an appropriate security clearance but who has not engaged a legal representative) to access the record or varied record of the NSI hearing and to prepare documents or records in relation to that record in a way and at a place prescribed by the regulations. The court must not give access to the record to anyone else.

963. Item 16 amends paragraph 38I(9)(a) to provide that access to the record of the closed hearing to a party or a party's legal representative will not be permissible where:

- the court has made an order under new subsection 38I(3A), or
- new paragraphs 38J(2)(e), 38J(3)(d) or 38J(4)(c) apply to exclude the subject of the control order and their legal representative from parts of the substantive control order proceeding in which information the subject of an order under revised section 38J is considered by the court.

**Item 17 – Subparagraph 38I(9)(a)(i)**

964. Item 17 is a minor consequential drafting amendment as a result of item 16. It does not change the effect of the provision.

**Item 18 – Subparagraph 38I(9)(a)(iii)**

965. Item 18 removes the reference to former section 38J (concerning a request to delay making a record or varied record available pending an appeal decision) which is repealed by Item 21 and replaced with new section 38J. The content of former section 38J is in new subsection 38I(10) (see item 19).

**Item 19 – At the end of section 38I**

966. Item 19 inserts new subsection 38I(10) which replicates the content of former section 38J. This ensures that all the primary provisions regarding the operation of closed hearings are contained within section 38I.

**Item 20 – Before section 38J**

967. Item 20 inserts a new heading of 'Subdivision B – Orders'. New Subdivision B will be located in Division 3 of Part 3A of the NSI Act. New Subdivision B deals with the new orders that will be available in control order proceedings as well as the existing orders under the NSI Act.

**Item 21 – Section 38J**

968. Item 21 repeals and substitutes existing section 38J. Former section 38J has been relocated to new paragraph 38I(10) (see Item 19).

969. New section 38J contains the substantive amendments to the NSI Act and creates three new types of orders. New subsection 38J(1) provides the circumstances under which one of the new orders can be made. Section 38J applies when:

- there is a proceeding under Division 104 of the *Criminal Code* in relation to a request to make a control order, an election to confirm a control order, or a request to vary a control order in relation to a person (the ***relevant person***) (the control order proceeding)
- the Attorney-General has issued a civil non-disclosure certificate or a civil witness exclusion certificate under sections 38F or 38H

- the Attorney-General has requested the court to make one of the new orders under subsection 38J(2),(3) or (4), and
- the court has held a closed hearing under subsection 38G(1) or 38H(6) for the purpose of determining whether to make one of the new orders under section 38J.

970. In determining whether to make an order under revised section 38J, the court must be satisfied that the subject of the control order (or proposed control order) has been given 'sufficient information about the allegations on which the control order request was based to enable effective instructions to be given in relation to those allegations'. This enables one or more of the allegations in the control order request to be supported by critical information—which may otherwise reveal sources, technologies and methodologies associated with gathering and analysing information—and for this information to be safeguarded under a section 38J order. However, procedural fairness requires that the person must still have notice of the allegations on which the application is based: sections 104.5(1)(h), 104.12A(2) and 104.23(3) of the *Criminal Code* provide minimum safeguards in relation to the information that must be provided. The court will consider all information provided to the person under those provisions and any other disclosure process which may apply to ordinary civil proceedings.

971. New subsection 38J(2) is the first new type of order a court may make for the purpose of a control order proceeding. New paragraph 38J(2)(a) provides that where the information is in the form of a document, the court may order that the information must not, except in permitted circumstances, be disclosed in the proceeding. However, under paragraph 38J(2)(b) a copy of the document with redactions may be disclosed, along with a summarised form of the national security information that has been redacted or a statement of facts that the information would or would be likely to prove.

972. New paragraphs 38J(2)(c) and (d) provide that the national security information may be disclosed to the court during the control order proceeding and, under such circumstances, the closed hearing rules under section 38I will apply.

973. New paragraph 38J(2)(e) provides that where national security information is disclosed during a closed hearing in the substantive control order proceeding, the relevant person and the relevant person's legal representative are not entitled to be present. The exclusion of the subject of the control order and their legal representative reflects the sensitivity of the information that is protected under a new subsection 38J(2) order.

974. New paragraph 38J(2)(f) provides that if the national security information in the document is disclosed during the control order proceeding and, apart from the order, the information is admissible in evidence in the proceedings, the court may consider the national security information, even if the information has not been disclosed to the relevant person or the relevant person's legal representative.

975. New subsection 38J(3) is the second type of new order a court may make for the purposes of a control order proceeding. It is applicable irrespective of the form of the national security information. The principal difference between the order under new subsection 38J(2) and new subsection 38J(3) is that under subsection 38J(3), information may be disclosed to the court and considered by the court for the purposes of a control order proceeding, without its contents being disclosed in any form to the relevant person or the

relevant person's legal representative. When this information is disclosed to the court, the closed hearing requirements under section 38I will apply.

976. New paragraph 38J(3)(d) operates in the same way as new paragraph 38J(2)(e). It provides that where the national security information is disclosed during the closed hearing in the substantive control order proceeding, the relevant person and the relevant person's legal representative are not entitled to be present. The exclusion of the subject of the control order and their legal representative reflects the sensitivity of the information that is protected under a new subsection 38J(3) order.

977. New subsection 38J(4) is the third type of new order a court may make for the purpose of a control order proceeding. New subsection 38J(4) provides that where a hearing is required under subsection 38H(6) in relation to the calling of a witness in the control order proceeding, the court may order that the relevant person and their legal representative must not call a witness at a hearing in the proceeding and that the closed hearing requirements under section 38I will apply if a witness is called at a hearing in the proceeding.

978. New paragraph 38J(4)(c) operates in the same way as new paragraphs 38J(2)(e) and 38J(3)(d). It provides that at any part of the substantive control order hearing in which the closed hearing requirements apply in relation to a witness who is to be called, the relevant person and the relevant person's legal representative are not entitled to be present if the witness is called. The exclusion of the subject of the control order and their legal representative reflects the sensitivity associated with an order under new subsection 38J(4).

979. In determining whether to make one of the three orders under section 38J, new subsection 38J(5) requires that the court must consider the factors outlined in new paragraphs 38J(5)(a)–(c). Unlike subsection 38L(8), there is no requirement that the court must provide greater weight to one of the listed factors above others.

980. New subsection 38J(6) provides that if a court makes an order under new subsections 38J(2), (3) or (4) in relation to an interim control order proceeding relating to the relevant person, that order will apply in relation to a proceeding for the confirmation of the control order in relation to that person. The purpose of this amendment is to clarify that orders under revised section 38J may carry through from an interim control order proceeding to a confirmation proceeding. This is because a confirmation proceeding is an extension of the interim hearing. The same allegations, and information to support those allegations, will be considered at both stages. This subsection avoids duplication of closed hearings in relation to the same national security information.

981. New subsection 38J(7) provides that where a court does not make any of the three orders under new section 38J in relation to a control order proceeding, it must make an order under existing section 38L.

**Item 22 – Subsection 38L(1)**

982. Item 22 amends subsection 38L(1) to provide that the court must make an order under section 38L unless an order under new subsections 38J(2) and 38J(4) has been made in relation to the disclosure of information in control order proceedings under Division 104 of the *Criminal Code*.

**Item 23 – At the end of subsection 38L(1) (note)**

983. Item 23 inserts a note that orders under new subsections 38J(2) and 38J(3) relate to the disclosure and consideration of information for the purposes of control order proceedings under Division 104 of the *Criminal Code*.

**Item 24 – At the end of subsection 38L(6)**

984. Item 24 amends subsection 38L(6) to provide that the court does not need to make an order under subsection 38L(6) if it has already made an order in relation to the calling of a witness under new subsection 38J(4).

985. Item 24 also inserts a note that new subsection 38J(4) allows the court to make an order about the calling of a witness in control order proceedings under Division 104 of the *Criminal Code*.

**Item 25 – Subsection 38M(1)**

986. Item 25 amends subsection 38M(1) to require the court to provide a written statement of reasons for making an order under revised section 38J. This statement must be given to the person who is the subject of the order, the parties, the parties' legal representatives and the Attorney-General and his or her legal representatives. Subsections 38M(2), (3) and (4) will continue to operate in their existing form. The effect of this is that the court must provide the Attorney-General and his or her legal representative the proposed statement of its reasons for making an order under revised section 38J. The Attorney-General or his or her legal representative may request the court to vary the proposed statement of reasons if the Attorney-General considers that the proposed statement will disclose information and the disclosure is likely to prejudice national security. The court must make a decision on this request.

**Item 26 – Section 38O**

987. Item 26 provides that orders made under new Subdivision B (i.e. an order under revised section 38J or an order under section 38L) do not come into force until the order ceases to be subject to appeal, and remains in force until it is revoked by the court.

**Item 27 – Subsections 38P(1) and (2)**

988. Item 27 amends subsections 38P(1) and (2) to provide that where orders are made under revised section 38J, the party who brought the proceedings and the party against whom the proceeding was brought may apply to the court to adjourn the proceeding. The adjournment is designed to give the party time to decide whether to appeal against the order under revised section 38J, to withdraw the proceeding (in the case of the party who brought the proceeding) or to appeal against the order, and if necessary, to make that appeal or withdrawal.

**Item 28 – Section 38R (heading)**

989. Item 28 amends the heading of section 38R to provide, in accordance with the amendment in item 29, that the same appeal rights in respect of orders made under section 38L apply in respect of orders made under revised section 38J.

**Item 29 – Subsection 38R(1)**

990. Item 29 amends subsection 38R(1) to provide that a party to a civil proceeding or the Attorney-General may appeal against any order of the court made under revised section 38J. This extends the appeal rights already provided for under subsection 38R(1) for orders made by the court under section 38L to the orders a court may make under revised section 38J.

**Item 30 – Section 47 (heading)**

991. Item 30 repeals the current heading in section 47 which states 'Report to Parliament on certificates given by Attorney-General etc' and instead renames the heading 'Annual report'. This is to clarify that following the amended reporting requirements under Item 31 below, it is not only certificates given by the Attorney-General that must be reported annually to Parliament, but also the number of orders made under revised section 38J and the number of special advocates appointed under new section 38PA of the NSI Act (see Item 43 of Part 2, Schedule 15).

**Item 31 – At the end of section 47**

992. Item 31 relates to the Attorney-General's annual reporting requirements under the NSI Act. Section 47 of the NSI Act requires that the Attorney-General must cause to be tabled before each House of Parliament, a report that outlines the number of certificates issued by the Attorney-General (or Minister appointed by the Attorney-General) under various provisions of the NSI Act.

993. Item 31 implements Recommendation 6 of the Committee advisory report. It requires that the Attorney-General, as part of his or her annual reporting obligations to Parliament, also annually report on:

- the number of orders under revised section 38J that were granted by the court, and
- the control order proceedings to which the orders granted by the court under revised section 38J relate.

994. This is an additional transparency and oversight measure, designed to enhance public confidence in the operation of revised section 38J.

**Item 32 – Application of amendments**

995. Item 32 relates to the application of the amendments contained in Part 1 of Schedule 15. Item 32 provides that the amendments contained in Part 1 apply to a civil proceeding that begins before or after the commencement of this Item. Accordingly, the amendments contained in Part 1 will apply to control order proceedings that have already commenced and irrespective of whether or not the NSI Act has been invoked.

***Public Interest Disclosure Act 2013***

**Item 33 – Section 8 (paragraph (f) of the definition of designated publication restriction)**

996. Item 33 amends paragraph (f) of section 8 of the PID Act to include orders made under revised section 38J in the definition of 'designated publication restriction'. The definition already includes orders made under sections 31 or 38L of the NSI Act. Designated

publication restrictions generally encompass information determined to require a particularly high degree of protection because it may prejudice, for instance, the safety of an individual. Orders under revised section 38J concern information of this nature, which if disclosed, is likely to prejudice national security. The disclosure scheme under the PID Act is not intended to undermine orders made under the provisions of the NSI Act.

## Part 2 – Special advocates

*National Security Information (Criminal and Civil Proceedings) Act 2004*

### Overview

997. The amendments contained in Part 2 of Schedule 15 provide for a special advocate to be involved where the Attorney-General seeks a new protective order under revised section 38J (see Part 1, Schedule 15). The creation of a special advocate role implements Recommendation 5 of the Committee advisory report.

998. For the purposes of Part 2, the following terms are used:

- a **controlee** is the subject (or proposed subject) of a control order and a party to the civil proceeding
- the **ordinary legal representative** is the legal representative who represents the controlee in parts of the control order proceedings in which they and the controlee have not been excluded
- an **NSI hearing** is the closed hearing under subsection 38G(1) or 38H(6) to determine if and how information should be disclosed in the proceedings
- the **substantive control order proceeding** is the substantive control order proceeding where the court determines whether to make, confirm or vary a control order in relation to the controlee, and
- the **sensitive national security information** is the 'information' disclosed by the Attorney-General to the special advocate under new subsection 38PE(2), which is the information the Attorney-General is seeking to protect under an order under revised section 38J, or has already obtained protection for as a result of an order under revised section 38J.

### A special advocate

999. A special advocate is a security-cleared lawyer who represents the interests of a party who has been excluded from parts of a proceeding. For the purposes of Part 2, the excluded party is the controlee. Accordingly, the special advocate will represent the interests of the controlee in parts of the control order proceeding in which they (and their ordinary legal representative) have been excluded. The parts of the control order proceedings from which the controlee (and their ordinary legal representative) may be excluded are:

- the NSI hearing, and
- the substantive control order proceeding where information that is the subject of an order under revised section 38J is being considered by the court (the relevant order under revised section 38J will automatically exclude the controlee and their ordinary legal representative from these parts of the control order proceeding, see new paragraphs 38J(2)(e), 38J(3)(d) or 38J(4)(c) in Item 21 of Part 1, Schedule 15).

1000. The special advocate may represent the interests of the controlee by:

- making submissions to the court at any part of a hearing in the proceeding in which the controlee and their ordinary legal representative are not entitled to be present

- adducing evidence and cross-examining witnesses at such a part of a hearing in the proceeding, and
- making written submissions to the court.

**The relationship between the special advocate and the controlee**

1001. The special advocate is not a legal representative of the controlee and is not a party to the proceeding. The special advocate does not have an ordinary lawyer-client relationship with the controlee because there are restrictions on the extent to which a special advocate can represent their interests. The most important of these restrictions is that once the special advocate has been provided with the sensitive national security information under new subsection 38PE(2), communication between the special advocate and the controlee (and their ordinary legal representative) is restricted and subject to authorisation by the court. Moreover, the special advocate cannot disclose the sensitive national security information to the controlee, which distinguishes the special advocate from an ordinary legal representative, who generally has an obligation of complete disclosure to his or her client.

1002. However, the unique relationship between the special advocate and the controlee reflects the delicate balance that must be struck between safeguarding the interests of the controlee and protecting highly sensitive national security information, the disclosure of which may adversely affect Australia's national security interests.

**Appointment of a special advocate**

1003. The court already has the inherent power to appoint a special advocate on an ad hoc basis if it considers it appropriate. The amendments contained in Part 2 do not limit that power. Instead, Part 2 provides a legislative framework for the appointment of a special advocate where the following circumstances arise:

- there is a control order proceeding under Division 104 of the *Criminal Code*
- the NSI Act has been invoked by the Attorney-General
- the Attorney-General has issued a civil non-disclosure certificate under section 38F or a witness exclusion certificate under section 38H, and
- either:
    - the Attorney-General has requested an order under revised section 38J and the court has already granted an order under new subsection 38I(3A) to exclude the controlee and their ordinary legal representative from the NSI hearing, or
    - an order under revised section 38J has been made, which automatically excludes the controlee and their ordinary legal representative from parts of the control order proceeding where information subject to the order is considered by the court.

1004. However, even where the above criteria are satisfied, the appointment of a special advocate remains at the discretion of the court. The provisions are designed to provide the court flexibility to conduct the control order proceedings in the manner it considers most appropriate.

1005. If the court determines that a special advocate is required, the controlee will be able to choose a special advocate. The court will appoint the special advocate requested by the controlee if it considers a special advocate necessary and none of the following factors apply:

- the special advocate requested would result in the proceeding being unreasonably delayed
- the special advocate requested would have an actual or potential conflict of interest, and
- the special advocate requested has knowledge of national security information and disclosure of that information would be likely to prejudice national security and in the circumstances, there is a risk of inadvertent disclosure of that information.

1006. If the court considers that a special advocate is necessary, but one of the three factors outlined above apply, the court may appoint a different special advocate to the one requested by the controlee.

**Communication restrictions on the special advocate and the controlee (and their ordinary legal representative)**

1007. An important element of the special advocate framework is the communication process between the special advocate and the controlee (and their ordinary legal representative).

*Communication prior to the special advocate receiving the sensitive national security information*

1008. Prior to receiving the sensitive national security information from the Attorney-General under new subsection 38PE(2), the special advocate will generally be able to communicate with the controlee (and their ordinary legal representative) without any restrictions imposed by the court. This is because there will generally be no sensitive national security information that the special advocate will inadvertently disclose to the controlee.

1009. In rare circumstances, the court may make an order that prohibits or restricts communications between the special advocate and the controlee (or their ordinary legal representative) prior to the receipt of the sensitive national security information by the special advocate. The order must be in the interest of national security and cannot be inconsistent with the NSI Act or regulations made under the NSI Act.

*Communication after the special advocate has received the sensitive national security information*

1010. Following the disclosure of the sensitive national security information by the Attorney-General to the special advocate under new subsection 38PE(2), communications from the special advocate to the controlee (and their ordinary legal representative) may only be in writing and can only occur with the authorisation of the court. Oral communications are prohibited.

1011. The court will forward on a proposed written communication from the special advocate to the controlee (or their ordinary legal representative) if it is satisfied that the

written communication is not likely to prejudice national security. In arriving at its decision, the court may consult with the Attorney-General. Where there has been a written communication authorised by the court from the special advocate to the controlee (or their ordinary legal representative), the court must provide the Attorney-General and the AFP with a description of that communication. However, that description must not disclose information that is the subject of legal professional privilege.

1012. The controlee (or their ordinary legal representative) may continue to communicate with the special advocate following the receipt of the sensitive national security information by the special advocate. However, all communications must be in writing, and in the case of the controlee, must go through their ordinary legal representative.

**Delayed commencement**

1013. The special advocates amendments in Part 2 will commence on a day to be fixed by Proclamation. If the amendments in Part 2 do not commence within the period of 12 months beginning on the day this Act receives the Royal Assent, those amendments shall commence on the day after the end of that period. Accordingly, while Part 1 of the amendments to the NSI Act contained in Schedule 15 will commence on the day after the Act receives the Royal Assent, the amendments to the NSI Act contained in Part 2 relating to special advocates will have a delayed commencement of up to 12 months.

1014. The delayed commencement ensures that sufficient time is provided to operationalise the special advocate role. This will include making appropriate regulations which will govern a range of matters including the process by which an individual serves as a special advocate, the remuneration of special advocates and conflicts of interests. It will also be necessary to ensure sufficient special advocates are available such that the controlee has a 'choice' of special advocates to choose from. These supporting regulations and administrative arrangements will be established as soon as practicable in order to operationalise the special advocates role swiftly.

1015. The delayed commencement of the special advocates amendments mean that the amendments contained in Part 1 will apply for up to 12 months before the special advocates role in Part 2 becomes operational. However, as noted by the Committee advisory report, nothing in the amendments contained in Parts 1 or 2 of Schedule 15 preclude the court from exercising its inherent powers to appoint a special advocate on an ad hoc basis if it considers it necessary.

**Impact of Schedule 15 on other protective measures**

1016. The amendments contained in Parts 1 and 2 of Schedule 15 do not limit the ability of parties to seek existing protective orders such as public interest immunity claims or non-publication orders.

1017. Similarly, Parts 1 and 2 of Schedule 15 will not limit the ability of parties to seek arrangements for civil proceedings about disclosures of national security information under existing section 38B. The purpose of section 38B is to allow the Attorney-General and the parties to the proceeding to agree to an arrangement about the disclosure of national security information at any point during the civil proceeding. The court may then make such orders as it considers appropriate to give effect to the arrangement. The purpose of these arrangements is to provide an alternative means for handling national security information,

thereby reducing the procedural requirements associated with protecting that information through the operation of the NSI Act and Regulations.

**Item 34 – Section 7**

1018. Section 7 contains definitions for the purposes of the NSI Act. Item 34 amends section 7 to include a 'special advocate' in the list of definitions. The definition of a 'special advocate' of a party to a civil proceeding is set out in new subsection 38PA(1).

**Item 35 – Section 17**

1019. Item 35 repeals and replaces the existing meaning of 'likely to prejudice national security' so that instead of referring to a 'disclosure of information', it says that 'something' is likely to prejudice national security if there is a real, and not merely a remote, possibility that it will prejudice national security.

1020. The purpose of this amendment is to ensure that a 'communication' between the special advocate and the controlee (and their ordinary legal representative) is captured within the meaning of 'likely to prejudice national security'. The term 'something' overcomes any uncertainty as to whether the term 'disclosure' contained in existing subsection 17(1) is expansive enough to capture such communications in light of the definition of 'disclose' in section 7.

1021. Accordingly, the new meaning of 'likely to prejudice national security' is broad enough to capture communications between the special advocate and the controlee (and their ordinary legal representative), as well as 'a disclosure of information' (under existing subsection 17(1)) and 'the contravention of a requirement' (under existing subsection 17(2)).

**Item 36 – Paragraph 38I(2)(d)**

1022. Item 36 amends the closed hearing requirements under section 38I. It inserts special advocates into subsection 38I(2) to ensure that the special advocate of the controlee can be present during the following closed hearings:

- the NSI hearing, and
- the substantive control order proceeding when information that is the subject of an order under revised section 38J is considered by the court.

1023. The controlee (and their ordinary legal representative) may be excluded from the NSI hearing where the court has made an order under new subsection 38I(3A). Where an order under revised section 38J has been made, the controlee (and their ordinary legal representative) will be excluded from parts of the substantive control order proceeding in accordance with new paragraphs 38J(2)(e), 38J(3)(d) or 38J(4)(c). In both situations, a special advocate (if appointed) may be present to represent the interests of the controlee.

1024. Where the controlee (and their ordinary legal representative) have been excluded from an NSI hearing, the special advocate may make submissions to the court of the kind outlined in subsection 38I(4). However, they will be making these submissions as part of the functions conferred upon them under new section 38PB.

**Item 37 – Subsection 38I(9) (heading)**

1025. Item 37 repeals the existing heading 'Access to the record by a party or party's legal representative' and replaces it with 'Access to the record by a party, legal representative or special advocate'. The reason for the inclusion of the special advocate in the heading is outlined in Item 38.

**Item 38 – After paragraph 38I(9)(a)**

1026. Current subsection 38I(5) states that the court must, either before or after it makes an order under section 38L, make a record of the closed hearing. Item 14 in Part 1 of Schedule 15 amends existing subsection 38I(5) to also include an order under revised section 38J.

1027. The court must then provide access to the record to a party who has the security clearance at a level considered appropriate by the Secretary (of the Attorney-General's Department) but who has not engaged a legal representative, or any party's legal representative who has been given a security clearance at the level considered appropriate by the Secretary. Subsection 38I(7) states that the Attorney-General must be provided a copy of the record so that he or she may request a variation of the record such that information, the disclosure of which is likely to prejudice national security, will not be disclosed. Under subsection 38I(8), the court must make a decision on the request of the Attorney-General (or his or her legal representative).

1028. Where a special advocate represents the interests of the controlee in the closed hearing, new paragraph 38I(9)(aa) provides that the special advocate will have access to the record of the hearing and will be provided the opportunity to prepare documents or records in relation to the record in a way and at a place prescribed by the regulations for the purposes of this paragraph.

**Item 39 – At the end of section 38M**

1029. Item 39 provides that under new subsection 38M(5), the court must give the special advocate the written statement of reasons for making an order under revised section 38J or an order under existing section 38L.

1030. The written statement of reasons for the making of an order is important so that the special advocate understands the reasoning of the court. This will also be useful for the special advocate in the event that the controlee or the Attorney-General wishes to appeal the making of an order. The reasons for making an order under revised section 38J are likely to be of interest to the controlee (and their ordinary legal representative), while the reasons for the making of a section 38L order are likely to be of interest to the Attorney-General in understanding the reasons why an order was not made under revised section 38J.

1031. Similar to the record of the hearing under subsection 38I(5), under subsection 38M(3) the Attorney-General may request that the court vary the written statement of reasons for making an order so that information that is likely to prejudice national security is not disclosed. Under subsection 38M(4), the court must make a decision regarding this request.

1032. The note to new subsection 38M(5) states that subsections 38M(2) to (4) do not apply to the statement of reasons the court gives to the special advocate. That is, the special advocate will be given the unvaried statement of reasons for the making of the order.

**Item 40 – Subsections 38N(1) and 38S(1)**

1033. Subsection 38N(1) provides that where the court makes an order under subsection 38M(4), the Attorney-General can request the court to delay giving the written statement of reasons to allow time for the Attorney-General to determine whether to appeal against the court's decision, and if the Attorney-General decides to appeal against the decision, the time to make the appeal. Existing subsection 38N(2) provides that the court must grant this request.

1034. Item 40 amends section 38N to ensure that there is no delay in providing the special advocate the written statement of reasons for the making of an order under revised section 38J or existing section 38L.

1035. Existing section 38S provides that the Attorney-General may appeal against a decision of the court under section 38M in relation to the variation of the written statement of reasons for making an order under revised section 38J or existing section 38L.

1036. Item 40 amends section 38S because the Attorney-General will not have the ability to appeal the provision of an unvaried statement of reasons to the special advocate.

**Item 41 – At the end of Division 3 of Part 3A**

**Subdivision C – Special advocates in control order proceedings**

1037. Item 41 contains the primary amendments in Part 2. These amendments are located under new Subdivision C of Division 3 of Part 3A of the NSI Act. These amendments outline the process for the appointment of a special advocate, specify the role of the special advocate in control order proceedings and govern how the special advocate fulfils their functions under this Subdivision.

**New section 38PA – Appointment of special advocate**

1038. The court has the inherent power to appoint a special advocate on an ad hoc basis where it considers it appropriate. The provisions contained in Part 2 do not limit this inherent power. Instead, Part 2 provides a legislative framework for the appointment of a special advocate under a specific set of circumstances.

1039. New subsection 38PA(1) provides the two criteria that must be satisfied in order for a court to appoint a special advocate.

1040. Firstly, under new paragraph 38PA(1)(a), the proceeding must be a control order proceeding under Division 104 of the *Criminal Code* relating to an application to the issuing court to make a control order, to confirm a control order or to vary a control order. Secondly, under new paragraph 38PA(1)(b), the court must have already made an order under new subsection 38I(3A) to exclude the controlee (and their ordinary legal representative) from the NSI hearing or have already made a new subsection 38J(2), (3) or (4) order which automatically excludes the controlee (and their ordinary legal representative) from parts of the substantive control order proceeding where the information subject to the order is considered by the court.

1041. Where either of the new paragraphs 38PA(1)(a) and (b) are not satisfied, the court cannot appoint a special advocate. New subsection 38PA(1) also inserts a note referring to new section 38PB, which outlines the functions of the special advocate.

1042. The appointment of a special advocate by the court is discretionary. Even where the criteria for the appointment of a special advocate under new subsection 38PA(1) are satisfied, the court may consider that the appointment of a special advocate is unnecessary. The provisions are designed to provide the court flexibility to conduct the control order proceedings in the manner it considers most appropriate. This will require the court to balance the need to conduct proceedings efficiently and effectively with the need to protect the procedural rights of the controlee.

1043. One instance in which the court may not appoint a special advocate even where the criteria outlined above have been satisfied is where the court considers itself adequately equipped to manage the sensitive national security information. Courts are not unfamiliar with considering sensitive national security information. The courts are well-equipped to make judgments as to the weight that should be given to the risk that disclosing information will prejudice national security.

1044. Accordingly, when the circumstances in subsection 38PA(1) are met, the court may make one of three decisions:

- the court may appoint a special advocate to represent the interests of the controlee in the NSI hearing as soon as it has made an order under new subsection 38I(3A)
- the court may choose not to appoint a special advocate to represent the interests of the controlee in the NSI hearing, even if it has made an order under new subsection 38I(3A), but may choose to appoint a special advocate to represent the interests of the controlee in the substantive control order proceedings where the sensitive national security information protected by an order under revised section 38J is being considered by the court, or
- the court may choose not to appoint a special advocate in either the NSI hearing or the substantive control order proceeding where the information subject to an order under revised section 38J is considered by the court.

1045. New subsection 38PA(2) provides that the court can only appoint a special advocate requested by the controlee if:

- the special advocate meets the requirements specified in the regulations to qualify as a special advocate, and
- the court has provided the parties to the proceeding (including the AFP (and the AFP's legal representative) and the controlee (and their ordinary legal representative)) and the Attorney-General (and the Attorney-General's legal representative) the opportunity to make submissions to the court about whom the court should appoint.

1046. The purpose of new subsection 38PA(2) is to ensure that any concerns the AFP or the Attorney-General may have with the appointment of the special advocate requested by the controlee can be put to the court. Some of the reasons the AFP or Attorney-General may advance for requesting the court to appoint a different special advocate to the one requested by the controlee are outlined in new paragraphs 38PA(3)(a)-(c). The controlee (and their

ordinary legal representative) will be provided with the opportunity to respond to the concerns of the AFP and the Attorney-General.

1047. New subsection 38PA(3) provides that the court may appoint a different special advocate to the one requested by the controlee only if the court is satisfied that:

- appointing the requested special advocate would result in an unreasonable delay to the control order proceeding (new paragraph 38PA(3)(a))
- appointing the requested special advocate would result in the special advocate having an actual or potential conflict of interest (new paragraph 38PA(3)(b)), or
- the requested special advocate:
    - has knowledge of national security information
    - the disclosure of the information would be likely to prejudice national security, and
    - in these circumstances, there is a risk of inadvertent disclosure of that information (new paragraph 38PA(3)(c)).

**New section 38PB – Function of special advocate**

1048. New section 38PB outlines the ways in which the special advocate may represent the interests of the controlee. The special advocate may represent the interests of the controlee by:

- making submissions to the court in any part of the control order proceeding where the controlee and their ordinary legal representative are not entitled to be present
- adducing evidence and cross-examining witnesses at such a part of the hearing in the control order proceeding, and
- making written submissions to the court.

**New section 38PC – Relationship of special advocate and relevant person**

1049. New section 38PC clarifies the nature of the relationship between the special advocate and the controlee.

1050. New subsection 38PC(1) states that the relationship between a special advocate and a controlee is not that of a legal representative and a client. Unlike a traditional lawyer-client relationship, the special advocate will have some restrictions on how they communicate with the controlee, including a complete prohibition on the special advocate revealing the sensitive national security information to the controlee.

1051. New subsection 38PC(2) states that despite the special advocate and controlee not being subject to a traditional lawyer-client relationship, legal professional privilege will apply to a communication between the special advocate and the controlee (and their ordinary legal representative) in the same way it would apply to a communication between a lawyer and client. This ensures that confidence inherent in communications between a lawyer and client are preserved when the special advocate communicates with the controlee (and their ordinary legal representative) (and vice-versa) in order to ensure frank and honest communication. In rare circumstances, the court, in consulting with the Attorney-General regarding a proposed

written communication from the special advocate to the controlee (or their ordinary legal representative) under new subsection 38PF(5), may choose to limit or abrogate legal professional privilege. However, this will only occur following a careful balancing of the competing interests by the court.

1052. New subsection 38PC(3) provides that the special advocate is not a party to a proceeding. This means that, for instance, if the special advocate considered that a court order (such as an order under revised section 38J) should be appealed, the special advocate must request the appeal be initiated through the ordinary legal representative of the controlee.

1053. New subsection 38PC(4) clarifies that for the purposes of the NSI Act, the special advocate is not a court official.

**New section 38PD – Communication before disclosure of information to special advocate by Attorney-General**

1054. New section 38PD governs communications between the special advocate and the controlee (and their ordinary legal representative) prior to the special advocate being provided the 'information' (i.e. the sensitive national security information) by the Attorney-General under new subsection 38PE(2).

1055. New subsection 38PD(1) provides that, except where new subsection 38PD(2) applies, communication between the special advocate and the controlee (and their ordinary legal representative) is not restricted under new Subdivision C prior to the Attorney-General disclosing the sensitive national security information to the special advocate under new subsection 38PE(2) in relation to the control order proceeding.

1056. The purpose of new subsection 38PD(1) is to ensure that up to the point of the Attorney-General providing the special advocate the sensitive national security information, the special advocate can communicate with the controlee (and their ordinary legal representative), in writing or orally without any restrictions imposed by the court, in much the same way as an ordinary legal representative would communicate with their client. This will provide the special advocate an opportunity to understand the open material and liaise with the controlee (and their ordinary legal representative) in order to gain context about the control order proceeding.

1057. However, new subsection 38PD(1) also inserts a note that provides that upon receipt of the sensitive national security information by the special advocate under new subsection 38PE(2), the communication restrictions contained in new section 38PF will apply.

1058. New subsection 38PD(2) provides that the court may make such orders as it considers appropriate prohibiting or restricting communications between the special advocate and the controlee (or their ordinary legal representative) about any matter connected with the control order proceeding if the court is satisfied that it is in the interest of national security to make such an order and if the order is not inconsistent with the NSI Act or regulations made under the NSI Act.

1059. The purpose of new subsection 38PD(2) is to allow the court to make orders prohibiting or restricting communication in circumstances where it is necessary for national security purposes to have such a prohibition or restriction. There may be instances where the special advocate has knowledge of national security information, potentially even the

sensitive national security information to be disclosed by the Attorney-General under new subsection 38PE(2). They may have acquired this information through other means such as another proceeding. In such instances, it is appropriate that the general rule in favour of communication without restriction between the special advocate and the controlee (or their ordinary legal representative) be prohibited or restricted.

**New section 38PE – Disclosure of information to special advocate by Attorney-General**

1060. New section 38PE relates to the disclosure of the sensitive national security information by the Attorney-General to the special advocate. The term 'disclose' is defined in section 7. The 'information' referred to in new section 38PE is the sensitive national security information which the Attorney-General:

- is seeking to protect through an order under revised section 38J – at this point the sensitive national security information will be subject to a relevant certificate given to the controlee (or their ordinary legal representative) under section 38F or 38H, or
- has obtained protection for as a result of an order under revised section 38J.

1061. That is, new subparagraphs 38PE(1)(a)(i) and (ii) cover different scenarios depending upon the point at which the court appoints a special advocate. If the special advocate is appointed prior to the NSI hearing, the special advocate will be provided the certificate under new subparagraph 38PE(1)(a)(i) and the statement of reasons for withholding the information from the controlee (and their ordinary legal representative) under new paragraph 38PE(1)(b).

1062. However, where the special advocate is not present at the NSI hearing but is only appointed by the court after the court makes an order under revised section 38J, the special advocate will only be provided the order made under new subsections 38J(2), (3) or (4). Under these circumstances, the special advocate will not need to be provided the certificate because the certificate will no longer be relevant.

1063. New subsection 38PE(2) provides that the Attorney-General must comply with the order of the court under new subsection 38PE(1). This means the Attorney-General must disclose to the special advocate the sensitive national security information pursuant to new subsection 38PE(1).

1064. New subsection 38PE(3) provides that the special advocate must not disclose (whether in the control order proceedings or otherwise) the sensitive national security information contained in the relevant certificate provided by the Attorney-General to the controlee (and their legal representative), or an order under revised section 38J, except in the circumstances provided for under new paragraphs 38PE(3)(a)-(c).

1065. The three circumstances under which the special advocate may communicate the sensitive national security information are:

- in permitted circumstances specified in the certificate given under section 38F or 38H, or in accordance with the order (if any) made under new subsections 38J(2), (3) or (4)
- to:
    - the AFP (or their legal representative), or

- the Attorney-General (or the Attorney-General's legal representative or any other representative of the Attorney-General), or

- to the court as part of the control order proceeding during which the controlee (and their ordinary legal representative) are not entitled to be present.

1066. The reasons for these exceptions are that under all three circumstances, the disclosure of the sensitive national security information is not likely to prejudice national security. In each situation, disclosure has either been approved (pursuant to a certificate or a relevant order under revised section 38J) or the individuals to whom the disclosure is made have already seen this information (as in the case of the AFP, the Attorney-General and the court).

1067. New subsection 38PE(3) also inserts a note that states that contravention of new subsection 38PE(3) by the special advocate is an offence under new subsection 46H(1). The operation of the offence in new subsection 46H(1) is discussed further below (see Item 42 of Part 2, Schedule 15).

1068. New subsection 38PE(4) provides that new paragraphs 38J(2)(a) and (3)(a) and existing subsections 38L(2) and (4) do not apply to the special advocate. Each of the mentioned paragraphs and subsections state that those whom a relevant certificate mentions, any persons to whom the contents of the certificate have been disclosed or any other specified person, must only disclose the information in permitted circumstances (or in accordance with the relevant subsection in the case of new paragraphs 38(J)(2)(a) and (3)(a)). These provisions do not need to apply to the special advocate because new subsection 38PE(3) already governs when and to whom the special advocate can disclose the sensitive national security information.

**New section 38PF – Communication after disclosure of information to special advocate by Attorney-General**

1069. New subsection 38PF(1) provides that new section 38PF applies after the Attorney-General has disclosed the sensitive national security information to the special advocate under new subsection 38PE(2) in the control order proceeding. The purpose of new section 38PF is to provide a framework to govern communications between the special advocate and the controlee (and their ordinary legal representative), and vice versa, following the receipt of the sensitive national security information by the special advocate.

1070. New section 38PF contemplates three communication scenarios:

- new subsection 38PF(2) captures communication between the special advocate and specific persons listed under that subsection

- new subsections 38PF(3)-(7) and new subsection 38PF(10) relate to communications by the special advocate to the controlee (or their ordinary legal representative), and

- new subsections 38PF(8) and (9) relate to communication by the controlee (and their ordinary legal representative) to the special advocate.

*Communication by the special advocate with specific persons*

1071. New subsection 38PF(2) provides that the special advocate must not communicate with any person about any matter connected to the control order proceedings, except the following individuals:

- the:
    - magistrate, judge or judges comprising the court
    - AFP (or the AFP's legal representative), or
    - Attorney-General (or the Attorney-General's legal representative or any other representative of the Attorney-General), or
- the controlee (or their ordinary legal representative) in accordance with new subsections 38PF(3), (4) or (10), or
- any other person if the communication is not about matters connected with the substance of the proceeding and the communication is necessary for administrative purposes.

1072. The special advocate may communicate with the above individuals without any authorisation from the court, or in the case of the controlee (or their ordinary legal representatives) subject to the requirements contained in new subsections 38PF(3), (4) or (10). New paragraph 38PF(2)(c) captures communications that are necessary for administrative purposes about matters not connected with the substance of the proceeding. This may include communication with court officials.

1073. New subsection 38PF(2) also inserts two notes.

1074. The first note provides that the special advocate will commit an offence under new subsection 46H(3) where he or she contravenes new subsection 38PF(2). The offence contained in new subsection 46H(3) is discussed further below (see Item 42 of Part 2, Schedule 15).

1075. The second note provides that the requirements under new subsection 38PF(2) will continue to apply to the special advocate after the end of the control order proceedings, or after the special advocate ceases to be a special advocate of the controlee. This is discussed further in new section 38PG.

*Communication by the special advocate with the controlee (or their ordinary legal representative)*

1076. New subsections 38PF(3)-(7) and new subsection 38PF(10) govern the communication of a special advocate with the controlee (or their ordinary legal representative). The overarching principle to these communications is that they must be in writing (i.e. oral communications are prohibited) and must occur only with the authorisation of the court (but for the limited exception for bare acknowledgements that is contained in new subsection 38PF(10)). While the restrictions on communications are necessary in order to protect sensitive national security information, they also provide a level of comfort for the special advocate. This is because having the court oversee any proposed written communications minimises the risk of inadvertent disclosure of sensitive national security information by the special advocate.

1077. New subsection 38PF(3) provides that a special advocate may submit a written communication to the court for approval and for forwarding to the controlee (or their legal representative).

1078. New subsection 38PF(4) gives the court three options when provided a written communication for approval and forwarding to the controlee (or their ordinary legal representative) by the special advocate.

1079. The first option, under new paragraph 38PF(4)(a), is that if the court is satisfied that the proposed communication is not likely to prejudice national security, it may forward that communication without making any amendments to the controlee (or their ordinary legal representative). The phrase 'likely to prejudice national security' is defined under revised section 17 (see Item 35 of Part 2, Schedule 15).

1080. The second option, under new paragraph 38PF(4)(b), is that if the court is not satisfied that the communication is not likely to prejudice national security, it may amend the communication to the extent necessary for the court to be satisfied it is no longer likely to prejudice national security. The court may then forward the amended communication to the controlee (or their ordinary legal representative).

1081. The third option, under new paragraph 38PF(4)(c), is that if the court is not satisfied that the communication is not likely to prejudice national security and the court is satisfied that it is not practicable to amend the communication so that it is not likely to prejudice national security, it must decline to forward the proposed communication to the controlee (or their ordinary legal representative) and notify the special advocate of that decision.

1082. New subsection 38PF(5) provides that the court may consult with the Attorney-General (or the Attorney-General's legal representative or any other representative of the Attorney-General) before making a decision regarding the proposed communication under new subsection 38PF(4). The option to consult the Attorney-General provides the court with an opportunity to seek the Attorney-General's views on the proposed communication. This reflects the fact that the Attorney-General, and agencies under his or her portfolio, have intimate knowledge of national security considerations and could provide the court with guidance in relation to why a proposed communication is likely to prejudice national security (or not likely to prejudice national security).

1083. New subsection 38PF(5) is not prescriptive as to how the court carries out the consultation process. The court may adopt whichever approach it considers appropriate in the circumstances. However, the court would likely try to ensure that legal professional privilege is protected to the greatest extent possible when consulting with the Attorney-General (or the Attorney-General's legal representative or any other representative of the Attorney-General).

1084. New subsection 38PF(6) provides that if the court forwards a written communication from the special advocate to the controlee (or their ordinary legal representative), the court must provide the AFP (or the AFP's legal representative) and the Attorney-General (or the Attorney-General's legal representative or any other representative of the Attorney-General) a description of the written communication. This ensures that the AFP and Attorney-General are notified of any communication between the special advocate and the controlee (or their ordinary legal representative) and are provided a general description of that communication.

1085. New subsection 38PF(6) should be read in conjunction with new subsection 38PF(7), which provides that the description provided to the AFP (or the AFP's legal representative) and Attorney-General (or the Attorney-General's legal representative or any other representative of the Attorney-General) must not disclose information that is the subject of

legal professional privilege. The purpose of this qualification is to ensure the confidentiality of communications between the special advocate and the controlee (or their ordinary legal representative) is maintained. This promotes honest communication between the special advocate and the controlee (or their ordinary legal representative).

*Communication by the controlee (or their ordinary legal representative) with the special advocate*

1086. New subsection 38PF(8) provides that the controlee may communicate with the special advocate about any matter connected with the control order proceeding. However, this communication must be in written form and occur through the controlee's ordinary legal representative. New subsection 38PF(8) inserts a note that states that the controlee commits an offence if he or she contravenes these requirements. The operation of the offence in new subsection 46H(4) is discussed further below (see Item 42 of Part 2, Schedule 15).

1087. New subsection 38PF(9) provides that the controlee's ordinary legal representative may communicate with the special advocate about any matter connected with the control order proceeding. However, this communication must only be in writing. New subsection 38PF(9) inserts a note that states that the ordinary legal representative of the controlee will commit an offence where he or she contravenes these requirements. The operation of the offence in new subsection 46H(5) is discussed further below (see Item 42 of Part 2, Schedule 15).

1088. The purpose of new subsections 38PF(8) and (9) is to clarify that once the special advocate has been provided the sensitive national security information by the Attorney-General under new subsection 38PE(2), the controlee (and their ordinary legal representative) can continue to communicate with the special advocate without any authorisation from the court. However, the communications must be in writing and in the case of the controlee, it must be done through the controlee's ordinary legal representative.

1089. New subsection 38PF(10) provides that when the controlee (or their ordinary legal representative) communicates with the special advocate in writing under either new subsections 38PF(8) or (9), the special advocate can send a bare acknowledgement of receipt of the written communication to the controlee (or their ordinary legal representative).

1090. New subsection 38PF(10) also inserts a note. The note provides that if the special advocate wants to communicate with the controlee (or their ordinary legal representative) beyond a bare acknowledgement of receipt of the written communication, the special advocate must submit a proposed written communication to the court for the court's approval in accordance with new subsections 38PF(3) and (4). The purpose of the note is to highlight that where a communication by the special advocate to the controlee (or their ordinary legal representative) is beyond a bare acknowledgement, then the court will need to assess whether the proposed written communication is likely to prejudice national security.

**New section 38PG – Communication after end of proceeding or by or to former special advocate**

1091. New section 38PG provides that the restrictions on communications under subsection 38PD(2), 38PE(3) and section 38PF (and offences for their contravention under new section 46H) continue to apply to the special advocate and the controlee (and their ordinary legal

representative) even if the control order proceeding has ended, or where the special advocate has ceased to act as the special advocate for the controlee.

1092. It is appropriate that any prohibition or restriction imposed upon communications between the special advocate and the controlee (and their ordinary legal representative) continue to apply even where the special advocate has ceased to act as a special advocate for the controlee, or the control order proceeding has ended. This is because the circumstances that gave rise to the prohibition or restriction continue to exist. For example, the risk of disclosure (including inadvertent disclosure) by the special advocate to the controlee is not mitigated simply because the proceedings have ended. The special advocate continues to have knowledge of sensitive national security information and as such, communication by or to the special advocate about any matter connected to the proceeding continues to pose a risk of prejudice to national security.

**New section 38PH – Hearings under subsection 38G(1) or 38H(6)**

1093. Existing section 15A of the NSI Act defines a 'civil proceeding'. Subsection 15A(2) provides that, to avoid doubt, each of the following is part of a 'civil proceeding':

(a) any proceeding on an ex parte application (including an application made before pleadings are filed in a court)

(b) the discovery, exchange, production, inspection or disclosure of intended evidence, documents or reports

(c) an appeal proceeding, and

(d) an interlocutory or other proceeding prescribed by regulations for the purposes of this paragraph.

1094. Subsection 15A(3) provides that, to avoid doubt, a re-hearing, and any proceeding relating to the re-hearing (including those mentioned in subsection 15A(2)), are part of the same civil proceeding as the hearing.

1095. The purpose of new paragraph 38PH(a) is to clarify that the NSI hearing is a hearing 'in' the control order proceeding under Division 104 of the *Criminal Code*. That is, the NSI hearing is part of the civil proceeding, being the control order proceeding. To the extent that this is unclear under existing section 15A, new paragraph 38PH(a) removes that uncertainty for the avoidance of doubt.

1096. This clarification is important because the role of the special advocate and the manner in which the special advocate carries out his or her functions depends to a large degree on the phrase 'in the proceeding' or matters 'connected with the proceedings'. For example, the special advocate can indeed represent the interests of the controlee in the NSI hearing because the NSI hearing is part of the proceeding.

1097. New paragraph 38PH(b) provides that any proceeding relating to an NSI hearing is also taken to be part of the civil proceeding, being the control order proceeding. This includes proceedings relating to an NSI hearing such as an appeal proceeding (for instance, an appeal following the making of an order under revised section 38J). In such a proceeding relating to an NSI hearing, the special advocate amendments, including those outlined above,

will apply, on the basis that the proceeding related to the NSI hearing is a proceeding that is part of the control order proceeding.

**New section 38PI – Regulations**

1098. New subsection 38PI(1) provides that the regulations may determine matters relating to special advocates. This is a broad power and ensures that Parliament has the requisite authority to make such regulations as necessary to ensure the effective operation of the special advocates role contained in new Subdivision C.

1099. Without limiting the scope of matters that might be encompassed in the regulations, new subsection 38PI(2) provides that the regulations may determine matters relating to the terms on which a person serves as a special advocate, including terms relating to remuneration, conflicts of interest or immunity.

1100. The amendments contained in Part 2 provide the architecture for the creation of a special advocate role in control order proceedings where the NSI Act is invoked and the new orders under revised section 38J are sought by the Attorney-General. Additional details, principally relating to the administrative arrangements necessary for the effective functioning of the special advocates role will need to be canvassed in regulations. These regulations will be established as soon as practicable in order to operationalise the special advocates role swiftly.

**Item 42 – At the end of Division 2 of Part 5**

**New section 46H – Offences relating to special advocates in control order proceedings**

1101. New section 46H provides for a range of offences relating to special advocates in control order proceedings.

1102. New subsection 46H(1) creates an offence for the disclosure of information by the special advocate. New subsection 46H(1) provides that the special advocate commits an offence if:

- the special advocate intentionally discloses sensitive national security information (whether in the control order proceeding or otherwise) they received from the Attorney-General under new subsection 38PE(2), and
- none of the exceptions for the disclosure of that sensitive national security information by the special advocate in new paragraphs 38PE(3)(a), (b) and (c) apply.

1103. The exceptions noted above refer to the exceptions under new subsection 38PE(3) relating to disclosure:

- in permitted circumstances or in accordance with the order under new subsections 38J(2), (3) or (4) (new paragraph 38PE(3)(a)),
- to the AFP (or the AFP's legal representative) (new subparagraph 38PE(3)(b)(i))
- the Attorney-General (or the Attorney-General's legal representative or another representative of the Attorney-General) (new subparagraph 38PE(3)(b)(ii)), or

- to the court as part of a hearing in the control order proceeding in which the controlee (and their ordinary legal representative) are not entitled to be present (new paragraph 38PE(3)(c)).

1104. These are circumstances in which the disclosure of the sensitive national security information is not likely to prejudice national security.

1105. New subsection 46H(2) provides that to avoid doubt, for the purposes of new subsection 46H(1), it does not matter whether the special advocate obtains the sensitive national security information in some way separate to that outlined under new subsection 38PE(2). One such alternative means may be through a separate proceeding in which the special advocate is involved. However, there is no exhaustive list of alternative means through which the special advocate may obtain that information. What is critical is the safeguarding of the sensitive national security information from disclosure in circumstances other than that permitted under new paragraphs 38PE(3)(a), (b) or (c).

1106. The disclosure of the sensitive national security information has the potential to disrupt ongoing law enforcement or intelligence operations, reveal technologies and methods used to collect and analyse intelligence, endanger the lives of human sources or adversely impact upon Australia's relationship with its international partners. Accordingly, a penalty of up to 2 years imprisonment is proportionate to the seriousness of the offence and mirrors existing penalties in the NSI Act for contraventions which may prejudice Australia's national security.

1107. New subsection 46H(3) creates an offence where there is a communication by a special advocate after the disclosure of sensitive national security information by the Attorney-General under new subsection 38PE(2). New subsection 46H(3) provides that the special advocate commits an offence if:

- the Attorney-General discloses the sensitive national security information to the special advocate under new subsection 38PE(2) in relation to the civil proceeding
- the special advocate intentionally communicates with another person about any matter connected with the proceeding
- the special advocate is reckless as to the circumstance that the communication occurs after the disclosure of the sensitive national security information to the special advocate under new subsection 38PE(2), and
- new paragraphs 38PF(2)(a), (b) and (c) do not apply to the communication.

1108. New subsection 38PF(2) states that the special advocate must not communicate with any person about any matter connected with the proceeding other than with:

- the:
    - magistrate, judge or judges comprising the court
    - AFP (or the AFP's legal representative), or
    - Attorney-General (or the Attorney-General's legal representative or any other representative of the Attorney-General), or
- the controlee (and their ordinary legal representative) in accordance with new subsections 38PF(3) and (4) or (10), or

- with any other person if the communication is not about matters connected with the substance of the proceeding and are necessary for administrative purposes.

1109. In order to represent the interests of the controlee, it is unlikely that the special advocate will need to communicate with anyone other than the individuals listed above about matters connected to the proceeding. There is an appropriate balance that has been struck between enabling the special advocate to carry out their statutory functions and ameliorating the risk of disclosure of sensitive national security information.

1110. The communication restrictions contained in new subsection 38PF(2) will continue to apply even after the control order proceeding has ended, or after the special advocate ceases to act as a special advocate for the controlee. The purpose of this offence is to ensure that any communication by the special advocate on any matter connected to the proceeding occurs only with the individuals identified in new paragraphs 38PF(2)(a), (b) and (c).

1111. The contravention of new subsection 46H(3) may result in imprisonment of up to 2 years.

1112. New subsection 46H(4) creates an offence relating to communication by the controlee to the special advocate after the disclosure of the sensitive national security information to the special advocate under new subsection 38PE(2).

1113. New subsection 46H(4) provides that the controlee commits an offence if:

- the controlee is or was a party to the control order proceeding
- the Attorney-General has disclosed the sensitive national security information to the special advocate under new subsection 38PE(2)
- the controlee intentionally communicates with the special advocate about any matter connected with the proceeding other than in writing through their ordinary legal representative, and
- the controlee is reckless as to the circumstance that the communication occurs after the special advocate has been provided the sensitive national security information under new subsection 38PE(2).

1114. The purpose of this offence is to ensure that the controlee only communicates with the special advocate in writing through their ordinary legal representative for matters that relate to the control order proceeding. The controlee must not orally communicate about any matter connected with the proceeding with the special advocate following the disclosure of the sensitive national security information to the special advocate by the Attorney-General under new subsection 38PE(2). This is because the special advocate is not able to communicate with the controlee other than with the approval of the court after this point (other than providing a bare acknowledgement in accordance with new subsection 38PF(10)). New subsection 38PF(8) not only protects the sensitive national security information, it also protects the special advocate from inadvertently disclosing sensitive national security information where the controlee wishes to communicate with them other than in writing through their legal representative (for instance, orally).

1115. This offence provision is designed to only affect the way the controlee communicates with the special advocate, as opposed to whether or when they can communicate with the special advocate. There are no restrictions on an controlee's ability to communicate with the

special advocate following the receipt of the sensitive national security information by the special advocate, other than that the communication must be in writing through their ordinary legal representative.

1116. This restriction continues irrespective of the control order proceeding having come to an end, or if the special advocate ceases to act as a special advocate for the controlee. The reason for this is that the special advocate will have already received the sensitive national security information under new subsection 38PE(2). Accordingly, there is a risk of inadvertent disclosure of that information to other persons, including the controlee, if communications are not undertaken by all persons in accordance with new section 38PF. This risk continues despite the control order proceeding having ended, or the special advocate ceasing to be the special advocate of the controlee.

1117. The contravention of new subsection 46H(4) may result in imprisonment of up to 2 years.

1118. New subsection 46H(5) creates an equivalent offence to new subsection 46H(4), except for the ordinary legal representative of the controlee.

1119. New subsection 46H(5) provides that the ordinary legal representative of the controlee commits an offence if:

- the Attorney-General has disclosed the sensitive national security information to the special advocate under new subsection 38PE(2) in relation to the control order proceeding
- the ordinary legal representative of the controlee intentionally communicates with the special advocate about any matter connected with the proceeding, other than in writing
- the ordinary legal representative is reckless as to the circumstance that the communication occurs after the special advocate has received the sensitive national security information under new subsection 38PE(2), and
- the ordinary legal representative is the ordinary legal representative of the party either:
    - at or after the time the disclosure of the information to the special advocate occurs under new subsection 38PE(2), and
    - at or before the time the communication occurs.

1120. The purpose of this offence is to prevent the ordinary legal representative communicating to the special advocate about any matter connected with the proceeding, other than in writing, following the disclosure of the sensitive national security information by the Attorney-General to the special advocate under new subsection 38PE(2). The ordinary legal representative of the controlee must not communicate orally with the special advocate after the special advocate has received the sensitive national security information.

1121. This restriction continues to apply even after the control order proceeding has ended, or the special advocate ceases to be the special advocate of the controlee in relation to the control order proceeding. The restriction is appropriate as it only applies in relation to communications about matters ‘connected with the proceeding’, being the control order proceeding. It is reasonable that such restrictions apply as there should be no need for the

ordinary legal representative of the controlee to communicate with the special advocate about any matter connected with the control order proceeding where the proceeding has ended, or the special advocate has ceased to be the special advocate for the controlee. Communication would only risk the likelihood of inadvertent disclosure of the sensitive national security information by the special advocate.

1122. The contravention of new subsection 46H(5) may result in imprisonment of up to 2 years.

**Item 43 – At the end of section 47**

1123. Item 43 inserts new paragraphs 47(e) and (f) in respect of the Attorney-General's annual reporting requirements. Section 47 of the NSI Act requires that the Attorney-General must cause to be tabled before each House of Parliament, a report that outlines the number of certificates issued by the Attorney-General (or Minister appointed by the Attorney-General) under various provisions of the NSI Act.

1124. Item 43 requires that the Attorney-General, as part of his or her annual reporting obligations to Parliament, must also annually report on:

- the number of special advocates appointed during the year under new section 38PA, and
- identify the control order proceeding under Division 104 of the *Criminal Code* in relation to which the special advocate(s) is appointed.

1125. This is an additional transparency measure, designed to enhance public confidence in the operation to the amendments contained in Parts 1 and 2 of Schedule 15. Given the Committee expressly recommended the creation of a special advocates role in respect of the amendments to the NSI Act contained in Part 1 of Schedule 15, it is important for Parliamentary oversight purposes to know how frequently special advocates are being appointed when the new orders under revised section 38J are obtained by the Attorney-General.

**Schedule 16— Dealing with national security information in proceedings**

***National Security Information (Criminal and Civil Proceedings) Act 2004***

1126. The NSI Act is complemented by the National Security Information (Criminal and Civil Proceedings) Regulation 2015 (the NSI Regulation) which prescribes, for the purpose of the NSI Act, the requirements for accessing, storing, handling, destroying and preparing security classified documents and national security information in proceedings to which the NSI Act applies.

1127. A common protection measure used under the NSI Act is an arrangement between parties (including the Attorney-General) about how to protect information in the proceeding. Where such an arrangement is made, the court can give effect to the arrangement by court order under subsection 22(2) or 38B(2) of the NSI Act. Where such an order is made, the NSI Regulation does not apply in relation to the information which is the subject of the order. This means that the parties and the Attorney-General can agree to depart from the NSI Regulation in relation to particular national security information in a proceeding. This may occur, for example, where the owner of the information is content for it to be stored in a manner different to that prescribed for in the NSI Regulation.

**Orders made under subsections 19(1A) and (3A)**

1128. A similar principle should apply in relation to orders made by the court under subsections 19(1A) and (3A) of the NSI Act. Subsections 19(1A) (Federal criminal proceedings) and (3A) (Civil proceedings) enable the court to make such orders as the court considers appropriate in relation to the disclosure, protection, storage, handling or destruction, in the proceeding, of national security information but only if the orders are not inconsistent with the NSI Act or the NSI Regulation.

**Proposed amendments – section 19**

1129. This Schedule amends section 19 to allow the court, on an application by the Attorney-General or a representative of the Attorney-General, to make an order enabling the parties to depart from the NSI Regulation in relation to particular national security information. This implements Recommendation 7 of the Committee advisory report.

**Orders made under subsections 22(2) or 38B(2)**

1130. Where the court gives effect to an arrangement between the parties and the Attorney-General about how to protect information in the proceedings under subsection 22(2) or 38B(2) of the NSI Act, the NSI Regulation does not apply to the information the subject of the court order (see subsections 23(2) and 38C(2)). In practice, this means that each order made under subsection 22(2) or 38B(2) must contain all the appropriate information protection measures covered by the NSI Regulation as the NSI Regulation will not apply once the order is made. This means, for example, that where the parties and the Attorney-General are content with the operation of most of the NSI Regulation but wish to depart from the NSI Regulation in respect of the storage of a particular document containing national security information, the court order under subsection 22(2) or 38B(2) must replicate all the other requirements provided for in the NSI Regulations.

**Proposed amendments – sections 23 and 38C**

1131. This Schedule amends sections 23 and 38C to enable the NSI Regulations to continue to apply to the extent they provide for ways of dealing with national security information that is disclosed, or is to be disclosed, in federal criminal proceedings and civil proceedings respectively.

**Item 1 – Paragraph 19(1A)(b)**

1132. This item repeals paragraph 19(1A)(b) and in substitution provides that in federal criminal proceedings the court may make such orders as the court considers appropriate in relation to dealing with national security information in the proceeding if (b) the orders are not inconsistent with the NSI Act and (c) the orders are not inconsistent with the NSI Regulations.

**Item 2 – After subsection 19(1A)**

1133. This item inserts paragraph 19(1B) which provides that paragraph 19(1A)(c) does not apply to orders made on an application by the Attorney-General or a representative of the Attorney-General. This means that these orders can be inconsistent with the NSI Regulations.

**Item 3 – Paragraph 19(3A)(b)**

1134. This item repeals paragraph 19(3A)(b) and in substitution provides that in civil proceedings the court may make such orders as the court considers appropriate in relation to dealing with national security information in the proceeding if (b) the orders are not inconsistent with the NSI Act and (c) the orders are not inconsistent with the NSI Regulations.

**Item 4 – After subsection 19(3A)**

1135. This item inserts subsection 19(3B) which provides that paragraph (3A)(c) does not apply to orders made on an application by the Attorney-General or a representative of the Attorney-General. This means that these orders can be inconsistent with the NSI Regulations.

**Item 5 – Subsection 23(2)**

1136. This item repeals subsection 23(2) and in substitution provides that the matters described in paragraphs 23(1)(a) or (b) apply in relation to national security information disclosed, or to be disclosed in a federal criminal proceeding only if there is not an order in force under section 22 relating to that information or there is an order in force under section 22 but the order does not deal with the matter. This means that the NSI Regulations continue to apply where an order is not in force under section 22 or continue to apply to the extent that the order in force under section 22 does not deal with the matter.

**Item 6 – Subsection 38C(2)**

1137. This item repeals subsection 38C(2) and in substitution provides that the matters described in paragraph (1)(a) or (b) of section 38C apply in relation to national security information disclosed, or to be disclosed in a civil proceeding only if there is not an order in

force under section 38B relating to that information or there is an order in force under section 38B but the order does not deal with the matter. This means that the NSI Regulations continue to apply where an order is not in force under section 38B or continue to apply to the extent that the order in force under section 38B does not deal with the matter.

**Item 7 – application and transitional provisions**

1138. This item provides that the amendments of sections 23 and 38B of the NSI Act made by this Schedule apply in relation to orders made on or after the commencement of this Schedule.

1139. This item also provides that the NSI Regulation, as in force immediately before the commencement of this Schedule, has effect on and after that commencement as if it had been made on that commencement. However, subsection 5(2) of the NSI Regulation does not have effect on or after that commencement, except in relation to orders made before that commencement.

1140. This item further provides that it does not prevent the amendment or repeal of the NSI Regulation.

**Schedule 17—Disclosures by taxation officers**

***Taxation Administration Act 1953***

**Item 1 – Subsection 355-65(2) in Schedule 1 (at the end of the table)**

1141. This item inserts a new item in Table 1 (Records or disclosures relating to social welfare, health or safety) at subsection 355-65(2) of Schedule 1 to the TA Act.

1142. Subject to legislated exceptions, section 355-25 of Schedule 1 to the TA Act creates an offence prohibiting the disclosure of protected information by taxation officers. The offence carries a maximum penalty of two years imprisonment. Table 1, at subsection 355-65(2) of Schedule 1 to the TA Act, sets out the exceptions to the offence provision for making a record of, or disclosing information relating to, social welfare, health or safety.

1143. This amendment creates an additional exception, authorising taxation officers to disclose information to an Australian government agency for the listed purposes. Those purposes are preventing, detecting, disrupting or investigating conduct that relates to a matter of security as defined by section 4 of the ASIO Act.

1144. Security as defined in the ASIO Act means:

(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from: espionage; sabotage; politically motivated violence; promotion of communal violence; attacks on Australia's defence system; or acts of foreign interference; whether directed from, or committed within, Australia or not; and

(aa) the protection of Australia's territorial and border integrity from serious threats; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

1145. The amendment will supplement existing exemptions and is designed to ensure that relevant information can be disclosed for listed purposes to Australian government agencies for the national security functions of the agency, including member agencies of the Australian Counter-Terrorism Committee and National Disruption Group, both of which have roles relating to the prevention, detection, disruption and investigation of terrorism and related conduct.

1146. By contrast, section 355-70 of Schedule 1 to the TA Act sets out the exceptions to the offence provision for disclosures relating to law enforcement and related purposes. The amendment in Item 1 is separate and distinct from the existing section 355-70, which requires there to be an investigation into a serious offence or the enforcement of a law, the contravention of which is a serious offence, or the making, or proposed, or possible making of a proceeds of crime order or supporting or enforcing such order. The amendment has been designed to allow disclosure for listed purposes to other Australian government agencies with national security functions, similar to the National Disruption Group, which may not yet exist. This ensures that Australian government agencies that are not currently member

agencies of national security bodies such as the National Disruption Group, but that could be represented on that Group at short notice, will be covered by the exception.

1147. A taxation officer will only be authorised to record or disclose the information for the purposes of preventing, detecting, disrupting or investigating conduct that relates to a matter of security. Conduct that relates to a matter of security within the meaning of the ASIO Act has the potential to affect the public (both in Australia and overseas) more generally rather than just a specific individual or group of individuals. For example, the commission of a terrorist act, financing a terrorist organisation or advocating terrorism online would all be considered as conduct that involves a matter of security.

1148. This new disclosure exemption recognises that the public interest in allowing government agencies to disclose information where this would, for example, prevent the commission of a terrorism offence and the resultant harm to an individual or to the public, outweighs the associated loss of privacy to the individual.

**Item 2 – After section 355-180 in Schedule 1**

1149. Item 2 implements Recommendation 20 of the Committee's advisory report by allowing an Australian government agency officer to disclose protected information to the Commonwealth Ombudsman.

1150. The Commonwealth Ombudsman has broad powers under section 9 of the Ombudsman Act to obtain information and documents relevant to an investigation. The amendment in item 2 has been created to ensure that officers of Australian government agencies who receive protected information for the purpose of preventing, detecting, disrupting or investigating conduct that relates to a matter of security as defined by section 4 of the ASIO Act can subsequently disclose that information to the Commonwealth Ombudsman for the purpose of the performance of his or her functions or duties under the Ombudsman Act and that the Ombudsman or their staff can record or disclose that same information for the same purpose.

1151. Item 2 has been drafted to align with existing national security disclosure exceptions in the law at section 355-185 of the TA Act, in relation to disclosure of protected information from ASIO to the IGIS for the purpose of the IGIS or their staff performing oversight duties in relation to ASIO or its employees.

1152. Subsection 355-182(1) of the TA Act creates an exception to the existing offence provision at section 355-155 of the TA Act for entities that make a record of information or disclose information to another entity (punishable by a maximum term of imprisonment of 2 years).

1153. Specifically, subsection 355-182(1) creates an exception to the existing offence at section 355-155 of the TA Act for an officer of an Australian government agency who discloses information to the Commonwealth Ombudsman where that information was acquired by the Australian government agency under the new exception provided by Item 1 above, and the record is made for, or the disclosure is to the Commonwealth Ombudsman, a Deputy Commonwealth Ombudsman, or a member of staff referred to in subsection 31(1) of the Ombudsman Act for the purposes of the performance, functions or duties by the Commonwealth Ombudsman.

1154. For example, where an Australian government agency has received taxpayer information for security purposes under the new exception at Item 1, the exception at subsection 355-182(1) would enable the entity to voluntarily disclose that information to the Commonwealth Ombudsman for the purposes of the functions or duties of that office without breaching section 355-155 of the TA Act.

1155. Subsection 355-182(2) creates a further exception to the offence at section 355-155 of the TA Act for the Commonwealth Ombudsman, Deputy Ombudsman or a member of staff referred to in subsection 31(1) of the Ombudsman Act who subsequently discloses information, where the information was acquired under either new subsection 355-182(1) or this new subsection 355-182(2), and the record or disclosure is made for the purpose of the performance of their duties under the Ombudsman Act.

1156. This ensures that any information received by the Commonwealth Ombudsman, a Deputy Commonwealth Ombudsman or a member of staff referred to in subsection 31(1) of the Ombudsman Act, can be used for the purpose of the performance of their functions or duties under the Ombudsman Act, including further disclosure for that purpose.

**Item 3 – Application**

1157. Item 3 provides that the amendment of the TA Act made by items 1 and 2 apply in relation to records and disclosures of information made on or after the commencement of this Schedule, regardless of whether that information was obtained before, on or after that commencement.

**Schedule 18**

***Australian Security Intelligence Organisation Act 1979***

**Overview**

1158. This Schedule amends section 35P of the ASIO Act to implement recommendations made by the INSLM in the INSLM report.

1159. These amendments will provide added protections by requiring that disclosures made by members of the community, except those who are entrusted persons, will only constitute an offence if the information will endanger the health or safety of a person or prejudice the effective conduct of a special intelligence operation (SIO). To achieve this, the existing offences in section 35P will be divided into two separate offence regimes, with one regime to apply to persons who came to the knowledge or into the possession of the relevant information in their capacity as an entrusted person (described in the INSLM's report as 'insiders') and a separate regime for persons where the information came to their knowledge or into their possession other than in the person's capacity as an entrusted person (described in the INSLM's report as 'outsiders'). An 'entrusted person' is defined in section 4 as an ASIO employee, an ASIO affiliate or a person who has entered into a contract, agreement or arrangement with ASIO (other than as an ASIO affiliate).

1160. These amendments will also include a defence of prior publication available only to persons who did not receive the relevant information in their capacity as an entrusted person.

1161. There will be four offences in total under the new section 35P regime: a basic offence and an aggravated offence for entrusted persons (who received the relevant information in their capacity as an entrusted person), and a basic offence and an aggravated offence for others. In addition to the offences in section 35P, an entrusted person will remain subject to the separate non-disclosure offence in section 18, and the related offences in sections 18A and 18B of the ASIO Act.

**Item 1 – Section 4**

1162. This item inserts a definition of 'entrusted person' into section 4 of the ASIO Act. An entrusted person who receives information in their capacity as an entrusted person will be subject to the new insider offences in section 35P. This definition currently appears in section 18A, and defines an entrusted person as an ASIO employee, an ASIO affiliate or a person who has entered into a contract, agreement or arrangement with ASIO (other than as an ASIO affiliate). The terms 'ASIO employee' and 'ASIO affiliate' are also defined in section 4.

**Consequential amendments (items 2 and 3)**

1163. These items remove the separate definitions of 'entrusted person' in subsections 18A(5) and 18B(5), to reflect that the definition will now be included in section 4.

**Item 4 – Subsections 35P(1) and (2)**

1164. This item repeals existing subsections 35P(1) and (2) and replaces them with four offences – a basic offence and an aggravated offence for entrusted persons (who received the

relevant information in their capacity as an entrusted person), and a basic offence and an aggravated offence for others.

1165. As with the existing provisions, the term 'disclose' is intended to take its ordinary meaning for the purpose of section 35P. It is intended to include the making available of information to others by any means. It is not intended to require, as a rule, proof that the information was received by another person, or proof that another person read, heard or viewed the information. Nor is the term intended to require proof that a person provided or intended to provide information to a particular person or group of persons.

1166. For each of the offences, the fault element in relation to whether the information disclosed relates to an SIO is recklessness. A person is reckless with respect to whether the information disclosed relates to an SIO if he or she is aware of a substantial risk that the information relates to an SIO and having regard to the circumstances known to him or her, it is unjustifiable to take that risk. Strict liability attaches to the physical elements of the offences in new paragraphs 35P(1)(a) and (1B)(a), as it would not be appropriate to require proof of recklessness in respect of these elements. For example, if a person has entered into a contract, agreement or arrangement with ASIO, proof of the existence of that contract, agreement or arrangement should be sufficient to establish this element of the offence.

*Disclosures by entrusted persons*

1167. New subsection 35P(1) sets out the basic offence for entrusted persons. This offence retains the elements found in existing section 35P(1), but will now only apply to a person who received the information in their capacity as an entrusted person. The maximum penalty for this offence is imprisonment for 5 years.

1168. New subsection 35P(1B) sets out the aggravated offence for entrusted persons. This contains the same elements as existing subsection 35P(2) and, like new subsection 35P(1), applies to a person who received the relevant information in their capacity as an entrusted person. The aggravated offence is distinguished from the basic offence by the existence of one or both of the following elements:

- the person intends to endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation
- the disclosure will endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation.

1169. The maximum penalty for this offence is imprisonment for 10 years.

*Other disclosures*

1170. The new offences in subsections 35P(2) and (2A) are intended to apply if the relevant information came to the knowledge or into the possession of the person other than in the person's capacity as an entrusted person. While it is envisaged this provision will apply primarily to members of the community who are not considered an entrusted person, the provision is not limited only to persons who are not and have never been an entrusted person. An entrusted person could still be subject to prosecution under subsection 35P(2) or (2A) if it was not demonstrated that they received the relevant information in their capacity as an entrusted person, although it is envisaged that this situation would be highly unusual.

1171. New subsection 35P(2) implements the INSLM's recommendation to establish a basic 'outsider' offence. It has the same elements as existing subsection 35P(1) but includes an additional harm requirement. New subsection 35P(2)(c) sets out a requirement that the disclosure of the information will endanger the health or safety of a person or prejudice the effective conduct of an SIO. The fault requirement for this element of the offence is recklessness. A person is reckless as to whether the disclosure of information will endanger the health or safety of any person or will prejudice the effective conduct of an SIO if he or she is aware of a substantial risk that such a circumstance exists or will exist, and having regard to that circumstance known to him or her, it is unjustifiable to take that risk.

1172. New subsection 35P(2A) establishes the corresponding aggravated offence for outsiders. This offence contains the same elements as existing subsection 35P(2) and new subsection 35P(1B). However, there is a higher fault element of knowledge, rather than recklessness, in relation to whether the disclosure will endanger the health or safety of any person or prejudice the effective conduct of an SIO. The maximum penalty for this offence is imprisonment for 10 years.

**Item 5 – Subsection 35P(3)**

1173. This item makes a consequential amendment to reflect the inclusion of new subsections. The exceptions to the offences set out in subsection 35P(3) will not be changed and will apply to both the entrusted persons and outsider offences.

**Item 6 – After subsection 35P(3)**

1174. This item implements the INSLM's recommendation for a defence relating to information that is already in the public domain. The defence will only apply to offences under subsections 35P(2) and (2A), and will therefore not apply to a disclosure by a person who received the relevant information in their capacity as an entrusted person.

1175. The new defence set out under subsection 35P(3A) specifies that the outsider offences (subsections 35P(2) and (2A)) will not apply to a person disclosing information, if the information has already been communicated or made available to the public (prior publication) and the person was not involved, directly or indirectly, in the prior publication. The defendant will bear the evidential burden and must adduce or point to evidence that suggests that the defendant believed, on reasonable grounds, that the disclosure would not endanger the health or safety of any person or prejudice the effective conduct of an SIO. Whether a belief is on reasonable grounds will depend, to an extent, on the nature, extent and place of the prior publication.

1176. The defence available under subsection 35P(3A) seeks to strike a balance between freedom of expression on the one hand, and recognition that further dissemination of harmful information could cause additional harm on the other hand. Before disclosing information that has already been published, a person must form a reasonable view that the subsequent disclosure will not cause additional harm. This is because in some cases, even where information is considered to have been published and in the public domain, subsequent disclosure will still result in harm. For instance, this would be the case where information is brought into the public domain inadvertently – such as where a classified document or information relating to an SIO is revealed as a result of technical or administration errors. Where steps are quickly taken to reverse the publication, subsequent mass disclosure of that

information is likely to bring that information to the attention of a much greater number of people and could result in considerable new or additional harm.

**Item 7 – Section 35P(4)**

1177. This item makes a consequential amendment to reflect the inclusion of new subsections.