2013-2014-2015

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

COUNTER-TERRORISM LEGISLATION AMENDMENT BILL (NO. 1) 2015

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Attorney-General, Senator the Honourable George Brandis QC)
COUNTER-TERRORISM LEGISLATION AMENDMENT BILL (NO. 1) 2015

GENERAL OUTLINE


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

FINANCIAL IMPACT STATEMENT

3. The measures in the Bill do not have a financial impact.
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 2015

4. The Counter-Terrorism Legislation Amendment Bill (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

Australian Security Intelligence Organisation Act 1979

5. 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. These amendments amend the ASIO Act to enable ASIO to furnish security assessments directly to states and territories.


6. 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”. These amendments amend 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

7. There are impediments to monitoring a person’s compliance with a control order imposed by an issuing court on the person. These amendments amend the Crimes Act to establish a new regime for monitoring the compliance of individuals the subject of a control order through monitoring search warrants, with a threshold targeted to monitoring. The Bill establishes complementary regimes for monitoring compliance with control orders under the TIA Act and SD Act.

8. 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. These amendments amend 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**

9. 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) and state police. 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 the receipt of funds for the purposes of 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 meaning of “imminence” for the purposes of obtaining a PDO.

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

10. The amendments to the NSI Act include:

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

11. There are impediments to monitoring a person’s compliance with a control order imposed by an issuing court on the person. The amendments to the SD Act establish a new regime for monitoring the compliance of individuals the subject of a control order through surveillance device warrants, with a threshold targeted to monitoring. The Bill establishes
complementary regimes for monitoring compliance with control orders under the Crimes Act and TIA Act.

12. Amendments to the SD Act will enable law enforcement officers to apply for a surveillance device warrant to monitor compliance with a control order. Further amendments will allow state or territory law enforcement officers to authorise the use of a tracking device without a warrant, to use an optical surveillance device or to use a listening or recording device in regards to a person subject to a control order in a manner consistent with the existing surveillance device framework.

13. The amendments specify the circumstances when protected information may be used, recorded, communicated or published in relation to a control order or a tracking device authorisation. In particular, the amendments enable law enforcement agencies to deal in protected information in connection with control order and PDO proceedings, in line with the AFP’s existing ability to use information obtained under the TIA Act in such proceedings.

**Taxation Administration Act 1953**

14. The TAA prohibits the disclosure of protected information by taxation officers unless one of the listed exceptions is satisfied. The amendments would create an additional exception to the offence provision, authorising taxation officers to 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.

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

15. As noted above, there are impediments to monitoring a person’s compliance with a control order imposed by an issuing court on the person. The amendments to the TIA Act establish a new regime for monitoring the compliance of individuals the subject of a control order with the terms of that order through telecommunications interception warrants. The Bill separately establishes complementary regimes for monitoring compliance with control orders under the Crimes Act and SD Act.

16. Amendments to the TIA will separately enable state and territory agencies to use lawfully intercepted information in 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**

**Australian Security Intelligence Organisation Act 1979**

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

17. 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.
18. “Security assessment” and “prescribed administrative action” are defined in section 35 and “security” in section 4.

19. The rights of notice and review will be unchanged. 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.

20. 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**

21. 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 on reasonable grounds suspect 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.

22. 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.

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

**Criminal Code Act 1995**

**Deletion of Family Court of Australia from definitions of “issuing court” and “superior court”**

24. 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.

25. The Family Court is also removed from the definition of “superior court” for the purposes of issuing a PDO. Present and former judges of superior courts are among those listed in section 105.2 who are able to be issuing authorities for PDOs. The remaining courts in the definition of “superior courts” are the High Court of Australia, the Federal Court, the Federal Circuit Court and state and territory Supreme Courts and District Courts.

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

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

27. The amendments to subsection 102.6(3) expands 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.

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

29. 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.

Definition of “advocates the doing of a terrorist act”

30. 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

31. 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.

32. 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.

33. 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, which can at its most serious include causing a person’s death, 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.

34. 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.

35. 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.

36. 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.
Monitoring warrants for control orders

37. 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.

38. The amendments create a “monitoring warrant” regime in a new Part IAAB of the Crimes Act to apply 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. Rather, this regime will target the monitoring of compliance with the conditions of a control order for the purposes of preventing a person from engaging in terrorist act planning or preparatory acts.

39. 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.

40. 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.

41. 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.

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

43. Article 17 of the ICCPR provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence.
44. 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.

45. 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.

46. 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.

47. 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.

48. 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.

49. 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.

50. 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 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.

51. 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 to a particular period. Authorised persons and any persons assisting them must leave the premises if the occupier withdraws consent.

52. 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.

53. 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

54. 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 penalty of seven years imprisonment.

55. 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.

56. The new offence is modelled on the recently enacted advocating terrorism offence in section 80.2C of the Criminal Code, but has some important differences that reflect the relevant international instruments. In particular, the new offence of advocating genocide is limited to public acts of advocacy.

57. The meaning of “advocates” in section 80.2D is consistent with that in subsection 80.2C(3), that is, “counsels, promotes, encourages or urges” 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.

58. 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.

59. 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.

60. 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 10 years imprisonment.

61. 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.

62. It is reasonable that genocide should not be publicly advocated and that reasonable steps should be taken to discourage behaviour that promotes such activity. Importantly, deterring the advocacy of genocide, which can at its most serious include causing a person’s death, 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.

63. 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.

64. 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.

65. 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.

66. 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.

67. A person charged with the offence of advocating genocide may be able to rely on the good faith defences in section 80.3, which protects 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.

68. 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

69. 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 is punishable, even without any of the genocide-related acts actually having been carried out.

70. 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

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

72. 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 on a person for the purpose of protecting the public from a terrorist act. 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.

73. 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 adults.

74. Subsection 104.28(2) builds upon the existing control order regime to allow an interim control order to be made 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 (10 years of age).

75. The lowering of the minimum age follows incidents, both in Australia and overseas, organised or led by children below the age of 16. 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 threshold of 16 years is no longer sufficient for control orders to prevent terrorist activity.

76. Control orders are one of the tools available to law enforcement authorities to prevent a person from carrying out terrorist acts. Children younger than 16 have shown themselves to be capable of participating in activity which poses a threat to national security, including participating in a terrorist act.

77. It should be noted that control orders are not a punitive measure but a preventative 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.

78. A control order does not authorise detention. A child 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 child’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 child 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.

79. The court can also require that the child 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.

80. The penalty for contravening a control order is five years imprisonment, regardless of whether the person is a child (of any age) or an adult (section 104.27). Prosecution for the offence would require proof that the child intentionally breached the relevant condition.
81. 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

82. 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.

83. Division 104 (Control Orders) of the Criminal Code will require the issuing court, when considering whether to impose the obligations, prohibitions and restrictions requested, to give consideration to the “best interests” of a person aged 14 to 17 years. 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.

84. 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 vulnerabilities are taken into account in determining their “best interests” before an interim control order is issued or confirmed. “Best interests” is consistent with Article 3.

85. 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, 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 child’s best interests as a primary consideration. New subsection 104.4(2A) treats the child’s best interests as “a primary” consideration.

86. For all control orders, regardless of the person’s age, the court must take into account the impact of the obligation, prohibition or restriction on the person’s circumstances, including their financial and personal circumstances (subsection 104.4(2)).

87. Where obligations, prohibitions and restrictions are imposed on the subject of the control order, paragraph 104.4(1)(d) the control 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.

88. As is the case now for 16 and 17-year-olds, control orders for all those aged 14 to 17 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)).

89. An important safeguard is that new section 104.28AA deals with court-appointed advocates for 14 to 17-year-olds. If the issuing court makes an interim control order in relation to the child, the court must as soon as practicable make an order appointing a lawyer to be the court-appointed advocate in relation to the interim control order, any proceedings relating to the confirmation of the control order, and any variation or revocation of the confirmed order. Section 104.28AA is modelled on sections 68L and 68LA of the Family Law Act, which provide for the appointment of an independent children’s lawyer. The significant differences are that the Family Court appointment is discretionary and the role of the independent lawyer is to be the child’s legal representative, whereas the issuing court is required to appoint an advocate who represents the child’s best interests.

90. The court-appointed advocate is not the child’s legal representative and is not obliged to act on the child’s instructions. The representative is not required to disclose to the court any information communicated by the child, but may disclose such information if the representative considers the disclosure to be in the child’s best interests, even if disclosure is against the child’s wishes.

91. The court-appointed advocate must form an independent view of what is in the best interests of the child, act in what the representative believes to be the child’s best interests, suggest to the court the adoption of a course of action which is in the best interests of the child, ensure any views expressed by the child in relation to the control order are fully put before an issuing court, and endeavour to minimise the distress to the child.

92. The interim control order, variations of the control order, a revocation of the control order and confirmations of the interim control order must be served on the court-appointed advocate (sections 104.12A, 104.17, 104.19, 104.20, 104.23 and 104.26). Reasonable steps must also be taken to serve those documents on at least one parent or guardian of the child (paragraph 104.12A(2)(c)).

93. The child may also have their own independent legal representation.

94. 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 the new subsection 104.4(2A), which 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.
95. A control order would only be issued against a child, especially one as young as 14, in the rare circumstance that it was required to prevent a child from being involved in a terrorist act. This includes protecting a child 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 child may be adversely affected if a control order is not issued in relation to that child. For example, the issuing of a control order in relation to a child may prevent the child’s contacting the group or individual who may be encouraging the child to engage in terrorist-related conduct.

96. However, Division 104 does not require that the imposition of the control order must be in the best interests of the child.

97. 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 children would not replace existing mechanisms such as those available under the Family Law Act to ensure children 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

98. Any combination of the obligations, prohibitions and restrictions listed in subsection 104.5(3) may be imposed as part of a control order:

   (a) a prohibition or restriction on the person being at specified areas or places

   (b) a prohibition or restriction on the person leaving Australia

   (c) a requirement that the person remain at specified premises between specified times each day, or on specified days

   (d) a requirement that the person wear a tracking device

   (e) a prohibition or restriction on the person communicating or associating with specified individuals

   (f) a prohibition or restriction on the person accessing or using specified forms of telecommunication or other technology (including the internet)

   (g) a prohibition or restriction on the person possessing or using specified articles or substances

   (h) a prohibition or restriction on the person carrying out specified activities (including in respect of his or her work or occupation)

   (i) a requirement that the person report to specified persons at specified times and places

   (j) a requirement that the person allow himself or herself to be photographed
(k) a requirement that the person allow impressions of his or her fingerprints to be taken

(l) a requirement that the person participate in specified counselling or education.

99. 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.

100. 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.

101. 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.

102. To the extent that there are any limitations placed on a young person’s human rights by the control order, these limitations must be reasonable, necessary and proportionate to achieving the legitimate objective of protecting the public from a terrorist act.

103. 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.

104. Article 14 provides that this freedom may be subject to such restrictions 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.

105. The restriction on being at particular places may engage the child’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 child report to specified persons at specified times and places.

106. 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 imposed limitations order on the people a child can associate if doing so was in the interests of national security or public safety and the rights and freedoms of others.
107. Imposition of a tracking device is one of the conditions that can be imposed by an issuing court as part of a control order. In relation to children aged 14 to 17 years, the issuing court would need to take into account whether it is in the child’s best interests to impose such a condition, noting the visible nature of a tracking device. As with all obligations, prohibitions and restrictions, the court could only impose this requirement, including the ancillary requirements in new subsection 104.5(3A), if it were reasonable necessary, and reasonably appropriate and adapted to achieving one of the purposes set out in Division 104.

108. Imposition of a tracking device on a child 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.

109. 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 child 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 child’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 child as young as 14 are likely to be limited.

110. 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.

111. 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.

112. Among the restrictions that may be placed on an individual – adult or child – 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.

113. The restriction on freedom of movement must be reasonable, necessary and proportionate to achieving this objective. These requirements are reflected in the legislative framework of the control order regime. An issuing court may only issue a control order where “the court is satisfied on the balance of probabilities that each of the obligations, prohibitions and restrictions to be imposed on the person by the order is reasonably necessary, and reasonably appropriate and adapted, for the purpose of protecting the public from a terrorist act” (paragraph 104.4(1)(d)). This ensures that the restrictions on freedom of movement caused by a control order are no greater than is required to protect the welfare of
the Australian public. The gravity of consequences likely to be occasioned by a terrorist act justifies a reasonable and proportionate limitation of free movement.

114. 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.

115. Each of the obligations, prohibitions and restrictions to be imposed on the person by the order 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
- preventing the provision of support for or the facilitation of the engagement in a hostile activity in a foreign country.

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

117. Control orders are used infrequently, with only six ever issued as at November 2015 (with none having been issued for people aged under 18 years of age). This reflects the policy intent that these orders do not act as a substitute for criminal proceedings. Control orders are a protective and preventative mechanism subject to numerous legislative safeguards that preserve the fundamental human rights of a person subject to a control order. The nature of the restrictions imposed by control orders will always be subject to the overarching legislative requirements that include consideration by the issuing court that any limitation is “reasonably necessary” and “reasonably appropriate and adapted” to protecting...
the public from a terrorist act. While there is an expectation that the number of control orders made will increase in coming years, the small number of control orders made to date and the small number relative to investigations and prosecutions reflects the policy intent that they are extraordinary measures which are to be used sparingly – and this is especially so with children.

**Preventative detention orders**

118. 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.

119. The amendments to the PDO regime contained in Schedule 5 are intended to clarify the operation of the “imminent” test in subsection 105.4(5) of the Criminal Code. The amendments achieve this by:

- adopting a new defined term of “imminent terrorist act”, and
- clarifying that the thresholds applicable to the AFP member and issuing authority under subsection 105.4(4) apply to the “imminent test in subsection 105.4(5).

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

120. 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.

121. The new defined term, “imminent terrorist act”, and the clarification of the applicable thresholds of “suspects, on reasonable grounds” for the AFP member and “reasonable grounds to suspect” for the issuing authority in satisfying the revised test of “imminent terrorist act” do not impact upon the right to freedom from arbitrary detention and arrest.

122. 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 suspect 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 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)).

123. 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 an imminent terrorist act occurring (paragraph 105.4(4)(c)) and that detention for the period specified is “reasonably necessary” for the purpose of preventing the imminent terrorist act (paragraph 105.4(4)(d)). This highlights the clearly preventative nature of the PDO power and creates a high threshold for its imposition. The combined operation of these criteria require that law enforcement agencies must make out a case for why the limitations imposed by the PDO are justified in each circumstance.

124. 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**

125. The amendments to the NSI Act contained in Schedule 15 provide for the enhanced protection of national security information in control order proceedings under Division 104 of the Criminal Code. Schedule 15 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 (or proposed subject) of the control order and their legal representative.

126. 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)).

127. The amendments to the NSI Act 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.

128. 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 some circumstances, the information will be so sensitive that
the existing protections under the NSI Act are insufficient. The inadvertent or deliberate
disclosure of such national security information may endanger the safety of individuals as
well as the general public, or jeopardise sources and other intelligence methods. In the
absence of the amendments contained in Schedule 15, a control order may not be able to be
obtained because of the inability to provide such information to the issuing court.

129. 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.

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

130. 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 (or proposed 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.

131. While the new orders provided under revised section 38J depart from ordinary
instances of procedure and judicial process, 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.

132. Firstly, 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 provided
sufficient notice of the allegations on which the control order request is based, even if the
individual may be denied notice of the information supporting those allegations. This ensures
that the subject (or proposed 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.

133. Secondly, 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)).

134. 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.

135. Thirdly, 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.

136. 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.

137. 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 (or proposed subject) of the control order has been afforded procedural fairness.

138. 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 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 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**

139. 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.

140. 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.

141. 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.

142. 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.

143. 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.

Right to life and security of the person in Articles 6 and 9 of the ICCPR

144. 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.

145. 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 characterised 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. Individuals and groups engaged in recently identified terrorism-related activities are proving more resistant to disruption than anticipated. 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, individuals returning to Australia
from particular conflict zones increase the likelihood of a terrorist attack in Australia due to their experiences fighting or training with proscribed terrorist groups.

146. 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 national security and 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.

147. Similarly, individuals returning to Australia from particular conflict zones increase the likelihood of a terrorist attack in Australia due to their experiences fighting or training with proscribed terrorist groups. Enhancing the surveillance capabilities of law enforcement agencies enables them to monitor ‘at risk’ individuals who have extensive links to terrorist groups, identify potential risks and intervene to prevent an act of terrorism.

148. The amendments to the SD Act allowing protected information to be dealt with in regards to control orders and PDOs assist national security and law enforcement agencies to prevent an act of terrorism from occurring.

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

149. 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.

150. 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.

151. 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. Individuals and groups engaged in recently identified terrorism-related activities are more resistant to disruption than anticipated. Also, 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.
The limited extension of the use of surveillance devices ensures that these amendments are reasonable and proportionate. Only people who are subject to a control order will have their right to privacy limited by these amendments. 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 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 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.

Under the current law, agencies have limited means for 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.

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.

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 obtain a warrant from an eligible judge or AAT member where the use or installation of a surveillance device requires entry into a premises or interference with a vehicle without the owner’s permission. Judicial 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.

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.

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.

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. This is a legitimate use of surveillance in light of the gravity of the terrorist threat.

159. 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.

160. 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.

161. 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 issued in control order and related proceedings.

162. 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*

163. 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 the purposes of national security or public order where such restrictions are provided by law and are clearly necessary.

164. 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 threat of terrorism is intensifying as it is becoming increasingly difficult for agencies to detect and disrupt attacks. In particular, individuals returning to Australia from particular conflict zones increase the likelihood of a terrorist attack in Australia due to their experiences fighting or training with proscribed terrorist groups. This heightened risk justifies any indirect limitation on free speech for a limited number of specific individuals subject to control orders.

Right to an Effective Remedy in Article 2(3) of the ICCPR

165. 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.

166. 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.

167. 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.

168. 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 officer engages in the conduct.

169. 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.

170. 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.

171. 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**

172. Subsection 355-65(2) of the TAA provides for disclosure of protected information for certain purposes relating to social welfare, health or safety. The amendment will supplement existing exemptions, authorising taxation officers to disclose 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. The amendment will only authorise the disclosure of protected information after commencement of the amendment.

173. Consistent with Item 9 of Table 1 at subsection 355-65 of the TAA, this amendment will authorise 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, as with bodies that have a role in preventing or reducing a serious threat to an individual’s life, health or safety or the public’s health or safety, bodies that have a role in preventing, detecting, disrupting or investigating a threat related to security 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.

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

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

175. Disclosure must be necessary or appropriate for purposes of preventing, detecting, disrupting or investigating conduct related to security. Disclosure 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. Information may only be disclosed to an agency for the
functions of that agency, including member agencies of the Australian Counter-Terrorism Committee and National Disruption Group. The disclosure is for a limited purpose and is neither arbitrary nor unlawful. Disclosures will only be able to be made after the provision commences, but the provision authorises disclosure of information collected before commencement of the Bill.

176. This exception to the non-disclosure provision only applies to situations where the public benefit associated with the disclosure clearly outweighs the need for taxpayer privacy. Agencies undertaking national security functions at any particular point in time will require the ability to acquire relevant information which would allow early intervention in terrorist activities, to prevent the possible widespread and devastating consequences of a terrorist attack.

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

177. 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).**

178. 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.

179. The Bill permits limited use of 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.

180. 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 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*

181. 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.

182. 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 characterised 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. Individuals and groups engaged in recently-identified terrorism-related activities are proving more resistant to disruption than anticipated. 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, individuals returning to Australia from particular conflict zones increase the likelihood of a terrorist attack in Australia due to their experiences fighting or training with proscribed terrorist groups.

183. 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 national security and 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.

184. Similarly, individuals returning to Australia from particular conflict zones increase the likelihood of a terrorist attack in Australia due to their experiences fighting or training with proscribed terrorist groups. 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.
185. The amendments allowing 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 privacy under Article 17 of the ICCPR

186. 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.

187. 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.

188. 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. Individuals and groups engaged in recently identified terrorism-related activities are more resistant to disruption than anticipated. Also, 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.

189. 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.
190. 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.

191. 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.

192. 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 will be able 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. First, the judge or nominated AAT member must have regard to the privacy of any person or persons 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.

193. The judge or AAT member must also have regard to what extent methods for these purposes listed above that do not involve intercepting communications have been used by or are available to the agency seeking the warrant, how much the use of such methods would be likely to assist or prejudice those purposes, and the possibility that the person subject to the control order:

- has engaged, is engaging, or will engage, in a terrorist act
- 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.

194. 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.

195. The Bill will enable state and territory agencies to use or communicate lawfully intercepted information in relation to their respective PDO regimes. Preventative detention orders 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.

196. 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.

197. 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.

198. 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 terrorist act or other related serious harm.
The right to freedom of expression in Article 19 of the ICCPR

199. 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 the purposes of national security or public order where such restrictions are provided by law and are clearly necessary.

200. 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 threat of terrorism is intensifying as it is becoming increasingly difficult for agencies to detect and disrupt attacks. In particular, individuals returning to Australia from particular conflict zones increase the likelihood of a terrorist attack in Australia due to their experiences fighting or training with proscribed terrorist groups. 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

201. 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.

202. 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.

203. 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.

204. 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.
205. 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.

206. 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.

207. 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

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

Clause 1 – Short title

210. This clause provides for the Bill to be cited as the Counter-Terrorism Legislation Amendment Act (No. 1) 2015.

Clause 2 – Commencement

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

212. 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. 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.

213. 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

214. 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)

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

216. 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.

217. “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.

218. 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.

219. Recommendation 20 of the Council of Australian Governments’ Review of Counter-Terrorism Legislation 2013 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. The Council of Australian Governments 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).

220. 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.

221. 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.

222. 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)

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

224. 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”.

225. 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**

227. 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 adults.

228. 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 (10 years of age).

229. These amendments respond to incidents in Australia and overseas that demonstrate children 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 which poses a threat to national security, the age limit of 16 years is no longer sufficient for control orders to prevent terrorist activity.

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

230. This item inserts a new definition of *court appointed advocate* in subsection 100.1(1) of the Criminal Code. Subsection 100.1(1) provides that a *court appointed advocate* has the meaning given by subsection 104.28AA(1).

**Item 2 – Paragraph 104.2(3)(b) of the Criminal Code**

231. 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).

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

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

234. 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 does not place any additional burden on the senior AFP member to obtain information about the proposed subject’s age.

235. 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.
236. This amendment differs from existing paragraph 104.2(3)(b) which requires that in seeking the Attorney-General’s consent for the interim control order, any information that the AFP member has about the person’s age must be given to the Attorney-General.

Item 3 – Paragraph 104.2(3) of the Criminal Code (note)

237. This item is consequential to the amendment to subsection 104.28 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 paragraph 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 4 – Paragraph 104.4(2) of the Criminal Code

238. This item amends subsection 104.4(2) by supplementing the existing requirement 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) with a more onerous requirement where the proposed subject of the control order is under 18 years of age.

239. That existing obligation is moved to new paragraph 104.4(2)(a) and applies in relation to all potential subjects of a control order.

240. In addition, new paragraph 104.4(2)(b) also requires the issuing court to take into account “the best interests” of the person when considering whether to impose each of the obligations, prohibitions and restrictions sought by the senior AFP member on a young person aged 14 to 17 years. This amendment will ensure that, in determining whether each of the obligations, prohibitions and restrictions to be imposed on the young person by the interim control order is reasonably necessary, and reasonably appropriate and adapted, the issuing court must take into account not only the impact of the obligation, prohibition or restriction on the person’s circumstances (including the person’s financial and personal circumstances) but also the best interests of the person. The additional 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.

Item 5 – After subsection 104.4(2) of the Criminal Code

241. This item inserts a new subsection 104.4(2A) in the Criminal Code after subsection 104.4(2). 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.

242. This list is adapted from the Family Law Act and is consistent with Australia’s international obligations under Article 3 of the Convention on the Rights of the Child.

**Item 6 – Subsection 104.5(1) of the Criminal Code (note 2)**

243. This item repeals existing Note 2 after subsection 104.5(1) and replaces it with a new Note 2, and reflects the reduction to the minimum age for a control order.

244. Existing Note 2 advises readers that a confirmed control order made in relation to a person aged 16 or 17 years must not end more than three months after the day on which the interim control order is made (see section 102.28).

245. New Note 2 advises readers that if an interim control order is imposed on a person aged 14 to 17 of two important matters. Firstly, the court must appoint a lawyer to be an independent advocate of the young person (see section 104.28AA). Secondly, 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 7 – Subparagraphs 104.12(1)(b)(vi) and (ix) of the Criminal Code**

246. This item amends subparagraphs 104.12(1)(b)(vi) and (ix).

247. 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.

248. Amended subparagraph 104.12(1)(b)(vi) will also require the AFP member to inform the subject of the right of their court appointed advocate (if relevant) to adduce evidence or make submissions to the issuing court in relation to the confirmation of an order.

249. Similarly, amended subparagraph 104.12(1)(b)(vi) will also require the AFP member to inform the subject of the right of their court appointed advocate (if relevant) to adduce evidence or make submissions to the issuing court in relation to an application to revoke or vary the confirmed order.

**Item 8 – Subparagraph 104.12(1)(b)(ix) of the Criminal Code**

250. This item is a technical amendment to subparagraph 104.12(1)(b)(ix) and removes the word “and” after the end of this subparagraph. This item is consequential to item 9 which inserts a new subparagraph 104.12(1)(b)(x) after existing subparagraph 104.12(1)(b)(ix).

**Item 9 – After subparagraph 104.12(1)(b) of the Criminal Code**

251. This item inserts new subparagraph 104.12(1)(b)(x) after existing subparagraph 104.12(1)(b)(ix).

252. New subparagraph 104.12(1)(b)(x) provides that if a control order is imposed on a young person aged 14 to 17 years, as soon as practicable after the interim control order is made and served on the young person, and at least 48 hours before the day specified in the
order for the confirmation hearing, the AFP member must inform the young person that he or she has a court appointed advocate and give the name and contact details of that advocate.

253. This is designed to ensure the young person has the option of contacting the appointed advocate for the purposes of discussing the order and obtaining advice. The role of the court appointed advocate of the child is set out in item 46 which inserts new section 104.28AA.

Item 10 – Subsection 104.12(5) of the Criminal Code (heading)

254. 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 11 – At the end of paragraph 104.12 of the Criminal Code

255. This item inserts a new heading “If person is 14 to 17” at the end of section 104.12.

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

257. New paragraph 104.12(6)(a) 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 personally serve a copy of the order on the person’s court appointed advocate. This is designed to ensure the court appointed advocate of a young person can appropriately undertake their legislative function as set out in new section 104.28AA.

258. New paragraph 104.12(6)(b) 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. This slightly lower requirement reflects the fact that 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. It 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 the inability to serve one of the young person’s parents or guardians with the order does not frustrate the commencement of the order.

259. 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.

Item 12 – Subparagraph 104.12A(2)(a)(iii) of the Criminal Code

260. 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.
261. The amendment clarifies that the requirement is to provide any other “written” details, acknowledging that it is not rational to require the AFP to provide details that are not in written form.

**Item 13 – At the end of subsection 104.12A(2) of the Criminal Code**

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

263. New subparagraph 104.12A(2)(c)(i) provides that, prior to the day specified in the order for the confirmation hearing, an AFP member must 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 the person’s court appointed advocate. This is designed to ensure the court appointed advocate of a young person can appropriately undertake their legislative function as set out in new section 104.28AA.

264. New paragraph 104.12A(2)(c)(ii) similarly provides that, 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. This slightly lower requirement reflects the fact that there will be instances where, even though the young person’s parents were able to be identified and located for the purposes of serving the initial order, it may not possible 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 the inability to serve one of the young person’s parents or guardians with the relevant documents does not prevent confirmation of the order.

**Item 14 – At the end of subsection 104.12A(4)(b) of the Criminal Code**

265. This item inserts new subparagraphs 104.12A(4)(iv) and (v).

266. 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.

267. Where the subject of the interim control order is a young person, new subparagraph 104.12A(4)(b)(iv) requires the AFP member to cause an annotated copy of the interim order, indicating that the order is no longer in force, as well as the notification that the AFP has elected not to confirm the interim control order, on the young person’s court appointed advocate.

268. In addition, where the subject of the interim control order is a young person, new subparagraph 104.12A(4)(b)(v) requires the AFP member to cause reasonable steps to be taken to cause an annotated copy of the interim order, as well as the notification that the AFP has elected not to confirm the interim control order, on the parent or guardian of the young person who was previously served.

269. These amendments are designed to ensure the person’s court appointed advocate (and in some instances the parent or guardian of the young person who was previously served) 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.
Item 15 – Before subsection 104.14(1) of the Criminal Code

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

271. 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.

272. 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.

273. 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, notification and service have been complied with.

Item 16 – Subsection 104.14(1) of the Criminal Code

274. 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 17 – Paragraph 104.14(1)(e) of the Criminal Code

275. 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). These words are unnecessary.

Item 18 – At the end of subsection 104.14(1) of the Criminal Code

276. This item inserts new paragraph 104.14(1)(f).

277. Existing subsection 104.14(1) sets out the individuals who may adduce evidence or make submissions to the issuing court in relation to the confirmation of the order.

278. New paragraph 104.14(1) provides that, where the subject of the interim control order is a young person aged between 14 and 17 years, the young person’s court appointed advocate may also adduce evidence or make submissions to the issuing court in relation to the confirmation of the order.

Item 19 – Subsection 104.14(4) of the Criminal Code

279. 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. The subsection has been revised to reflect the role of the court appointed advocate where the control order applies to a young person.

280. 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, the Queensland public interest monitor (if relevant), nor the court appointed advocate (if relevant) attend the court on the specified day.

**Item 20 – At the end of subsection 104.14(5) of the *Criminal Code***

281. This item adds a new paragraph 104.14(5)(d).

282. Existing subsection 104.14(5) provides that the issuing court may declare the interim order void, revoke the order, confirm and vary the order, or confirm the order without variation where any of the relevant criteria in subsections 104.14(6) of (7) are satisfied.

283. New paragraph 104.14(5)(d) provides that the issuing court may take those actions where the subject of the control order, a representative of the subject, the Queensland public interest monitor (if relevant), and/or the court appointed advocate (if relevant) attend the court on the specified day.

**Item 21 – Subsection 104.16(1) of the *Criminal Code* (note)**

284. This item repeals and replaces the note to subsection 104.16. The new note advises readers 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 22 – Subparagraph 104.17(1)(b)(iii) of the *Criminal Code***

285. This item amends subparagraph 104.17(1)(b)(iii) by including the words “or the person’s court appointed advocate” after the word “monitor”.

286. Current subparagraph 104.17(1)(b)(iii) specifies the individuals who the AFP must inform of the variation of an interim control order (with or without variation) by an issuing court. The amendment also requires the AFP to inform the young person that his or her court appointed advocate can adduce evidence or make submissions in relation to an application to revoke or vary the order.

**Item 23 – At the end of section 104.17 of the *Criminal Code***

287. This item adds a new heading “If person is 14 to 17 years” and a new subsection 104.17(4) to existing section 104.17.

288. Existing section 104.17(4) sets out the requirements in relation to service of a declaration, revocation, variation or confirmation of an interim control order.

289. 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 certain steps.
Specifically, new paragraph 104.17(4)(a) requires an AFP member to serve a copy of the declaration, revocation or confirmed control order personally on the young person’s court appointed advocate. In addition, new paragraph 104.17(4)(b) requires an AFP member to take reasonable steps to personally serve a copy of the order on the parent or guardian of the young person who was previously served.

Item 24 – Paragraph 104.18(4)(e) of the Criminal Code

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 25 – At the end of subsection 104.18(4) of the Criminal Code

This item adds a new paragraph (f) at subsection 104.18(4) to include the court appointed advocate of the young person aged 14 to 17 years, as one of the persons who may adduce additional evidence or may make additional submissions to the court, in relation to an application to revoke or vary a control order.

Item 26 – At the end of subsection 104.19(2) of the Criminal Code

This item adds new paragraph 104.19(2)(c).

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

Where the control order relates to a person aged 14 to 17 years, new paragraph 104.19(2)(c) also requires the AFP Commissioner to give written notice of the application and grounds for the application for revocation or variation of an order to the young person’s court appointed advocate.

Item 27 – After subsection 104.19(2) of the Criminal Code

This item inserts new subsection 104.19(2A).

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 of vary an order.

New subsection 104.19(2) provides that, where the subject of the control order is aged from 14 to 17 years, the AFP Commissioner is also required to notify the court appointed advocate and take reasonable steps to notify the parent or guardian of the young person who was previously served. New subsection 104.19(2) also requires the AFP Commissioner to serve a copy of the application and grounds on the court appointed advocate and take reasonable steps to serve those documents on the parent or guardian of the young person who was previously served.
Item 28 – Paragraph 104.19(3)(e) of the Criminal Code

299. 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). Those words are unnecessary.

Item 29 – At the end of subsection 104.19(3) of the Criminal Code

300. This item adds new paragraph 104.19(3)(f).

301. Existing subsection 104.19(3) specifies the individuals who may adduce additional evidence or make additional submissions to the issuing court in relation to an application to revoke or vary a confirmed control order.

302. Where the subject of the confirmed control order is a person aged 14 to 17 years, new paragraph 104.19(3)(f) provides that the person’s court appointed advocate can also adduce additional evidence or make additional submissions to the court in relation to an application to revoke or vary a control order.

Item 30 – Subsection 104.20(3) of the Criminal Code

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

304. 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.

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

306. Where the subject of the control order is aged 14 to 17 years, new subparagraph 104.20(3)(b)(i) also requires the AFP member to personally serve a copy of the revocation or variation on the person’s court appointed advocate. This is designed to ensure the court appointed advocate of a young person can appropriately undertake their legislative function as set out in new section 104.28AA.

307. In addition, where the subject of the control order is aged 14 to 17, new subparagraph 104.20(3)(b)(ii) provides that the AFP member must take reasonable steps to personally serve a copy of the revocation or variation on the parent or guardian of the young person who was previously served.

Item 31 – Paragraph 104.23(2)(d) of the Criminal Code

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

309. 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.

310. 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.
311. 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 person’s age.

Item 32 – Subsection 104.23(2) of the Criminal Code (note 1)

312. 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.

313. The new Note advises readers 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 33 – Subsection 104.23(3) of the Criminal Code

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

315. 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.

316. As soon as practicable after an application is made, new subsection 104.23(3) requires the Commissioner to personally serve the documents mentioned in new subsection 104.23(3AA) on the person subject to the order (paragraph 104.23(3)(a)), the Queensland public interest monitor (if relevant) (paragraph 104.23(3)(b)) and the court appointed advocate (subparagraph 104.23(3)(c)(i)). In addition, subparagraph 104.23(3)(b)(ii) requires that the AFP Commissioner take reasonable steps to personally serve the specified documents on the parent or guardian of the young person who was previously served (if relevant).

317. 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 34 – Subsection 104.23(3A) of the Criminal Code

318. 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 35 – Paragraph 104.23(4)(e) of the Criminal Code

319. 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). Those words are unnecessary.

Item 36 – At the end of subsection 104.23(4) of the Criminal Code

320. This item inserts a new paragraph 104.23(4)(f) after existing 104.23(4)(e).

321. Existing subsection 104.23(4) specifies the individuals who may adduce additional evidence or make additional submissions to the issuing court in relation to an application to vary a control order.

322. Where the subject of the control order is a person aged 14 to 17 years, new paragraph 104.23(4)(f) provides that the young person’s court appointed advocate may adduce additional evidence or make additional submissions to the issuing court in relation to an application to vary a control order.

Item 37 – Subsection 104.24(2) of the Criminal Code

323. This item amends subsection 104.24(2) by supplementing the existing requirement for an issuing court to take into account the impact of any additional obligation, prohibition or restriction on the person’s circumstances (including the person’s financial and personal circumstances) with a more onerous requirement where the subject of the control order is under 18 years of age.

324. That existing obligation is moved to new paragraph 104.24(2)(a) and applies in relation to all subjects of a control order.

325. In addition, new paragraph 104.24(2)(b) also requires the issuing court to take into account “the best interests” of the person when considering whether to impose each additional obligation, prohibition and restriction on a young person aged 14 to 17 years. This amendment will ensure that, in determining whether each additional obligation, prohibition and restriction to be imposed on the young person by the varied control order is reasonably necessary, and reasonably appropriate and adapted, the issuing court must take into account not only the impact of the obligation, prohibition or restriction on the person’s circumstances (including the person’s financial and personal circumstances) but also the bests interests of the person. The additional requirement for the court to consider the best interests of the young person aged from 14 to 17 years is consistent with Article 3 of the CRC and is adapted from the Family Law Act.

Item 38 – After subsection 104.24(2) of the Criminal Code

326. This item inserts a new subsection 104.24(2A) in the Criminal Code after subsection 104.24(2). 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.

327. This list is adapted from the Family Law Act and is consistent with Australia’s international obligations under Article 3 of the Convention on the Rights of the Child.

Item 39 – Subparagraph 104.26(1)(c)(v) of the Criminal Code

328. This item amends subparagraph 104.26(1)(c)(v).

329. Existing subsection 104.26(1)(c) sets out the requirements imposed on an AFP member after a control order is varied under section 104.24.

330. Where the subject of the control order is aged 14 to 17 years, new subparagraph 104.26(1)(c)(v) also requires an AFP member to inform the young person that the court appointed advocate has the right to adduce evidence or make submissions in relation to an application to revoke or vary the order.

Item 40 – At the end of section 104.26 of the Criminal Code

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

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

333. 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 serve a copy of the order personally on the person’s court appointed advocate and take reasonable steps to serve the order on the parent or guardian of the young person who was previously served.

Item 41 – Subdivision H of Division 104 of Part 5.3 of the Criminal Code (heading)

334. 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 42 – Subsection 104.28(1) of the Criminal Code (heading)

335. 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 43 – Subsection 104.28(1) of the Criminal Code**

336. This item amends existing subsection 104.28(1) by replacing the reference to “16” with “14”.

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

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

**Item 44 – Subsection 104.28(2) of the Criminal Code (heading)**

339. 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 45 – Subsection 104.28(2) of the Criminal Code**

340. 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”.

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

**Item 46 – After section 104.28 of the Criminal Code**

342. This item inserts new section 104.28AA after existing section 104.28.

343. New section 104.28AA provides for the appointment, role and limits on the disclosure of information in relation to the court appointed advocate.

344. After an issuing court makes an interim control order in relation to a young person aged 14 to 17 years, new subsection 104.28AA(1), “Appointment”, requires the issuing court to make an order appointing a lawyer to be the court appointed advocate of the young person as soon as practicable.

345. New paragraph 104.28AA(1)(a) provides that the court appointed advocate of the person is appointed in relation to the control order matters set out in new paragraphs 104.28AA(1)(a)(i) and (ii). Those matters are the interim control order and any proceedings under Division 104 relating to confirmation, variation or revocation of the order.

346. New paragraph 104.28AA(1)(b) gives the issuing court authority to make any other orders it considers appropriate to secure independent advocacy for the young person in relation to the control order matters.

347. The “Role” of the court appointed advocate is set out in new subsection 104.28AA(2).
New paragraph 104.28AA(2)(a) provides that the role requires the court appointed advocate to ensure, as far as practicable in the circumstances, that the young person understands the effect and period of the order, the person’s right to an appeal and review, right to attend court on the day specified, the right of the person or the person’s representative to adduce evidence or make submissions if the order is confirmed, and the person’s right to apply for an order revoking or varying the order if it is confirmed. The provision acknowledges that the court appointed advocate’s ability to ensure the young person understands these matters will be subject to the young person’s age, language skills, mental capacity and other relevant factors.

New paragraph 104.28AA(2)(b) requires the court appointed advocate to form an independent view, based on the evidence available to the advocate, of what is in the best interests of the person, and new paragraph 104.28AA(2)(c) requires the advocate to act in the what he or she believes to be the best interests of the young person. New paragraph 104.28AA(2)(d) requires the advocate to make a submission to an issuing court suggesting the adoption of a particular course of action if he or she is satisfied that the adoption of the particular course of action is in the best interests of the young person. New paragraph 104.28AA(2)(e) requires the court appointed advocate to ensure that any views expressed by the young person in relation to the control order matters are fully put before an issuing court. Finally, new paragraph 104.28AA(2)(f) requires the court appointed advocate to endeavour to minimise any distress to the young person associated with the control order matters.

Consistent with these provisions, new subsection 104.28AA(3) specifies that the court appointed advocate is not the young person’s legal representative and is not obliged to act on the instructions of the child. Rather, the advocate is an independent party who is responsible for representing the young person’s best interests rather than the expressed wishes of the young person. As with any person subject to a control order, the young person may separately obtain legal representation or other assistance in relation to the control order.

New subsections 104.28AA(4), (5) and (6) deal with issues relevant to the “Disclosure of information”.

New subsection 104.28AA(4) provides that the court appointed advocate of a young person is not obliged to disclose and cannot be required to disclose to an issuing court, any information that the young person communicates to the advocate. This is designed to facilitate a relationship of trust and open communication between the young person and the advocate.

However, new subsection 104.28AA(5) provides that the court appointed advocate may disclose information communicated by the young person to an issuing court if he or she considers the disclosure to be in the best interests of the person. This is designed to ensure information that could, for example, demonstrate that a person, including the young person subject to the control order, is in danger, can be disclosed and acted on appropriately. New subsection 104.28AA(6) provides that the advocate can make a disclosure to an issuing court under subsection 104.28AA(5) even if the disclosure is made against the wishes of the young person.
Item 47 – Before section 104.28A of the *Criminal Code*

354. This item inserts a new heading “Subdivision I—Miscellaneous” before section 104.28A.

Item 48 – At the end of subsection 104.29(2) of the *Criminal Code*

355. This item inserts new paragraph 104.29(2)(g).

356. 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 on 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”.

357. 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 in relation to persons aged 14 to 17 years.
Schedule 3—Control orders and tracking devices

Criminal Code Act 1995

Overview

358. A control order imposed by an issuing court under Division 104 of Part 5.3 of the Criminal Code empowers an issuing court to impose a requirement that the person subject to the order wear a tracking device. Where an issuing court imposes such a requirement as part of a control order, these amendments will place an obligation on the subject to ensure the tracking device remains operational and functional. These amendments respond to concerns that, if no such obligations are imposed, the subject could allow the device to go flat or could damage the device, making it ineffective.

Item 1 – After subsection 104.5(3)

359. This item inserts new subsection 104.5(3A) after subsection 104.5(3).

360. 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.

361. The requirements in new subsection 104.5(3A) 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). 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 are designed to ensure the utility of a requirement to wear a tracking device, where the wearing of a tracking device is deemed reasonably necessary for, and reasonably appropriate and adapted to, the protective and preventative function of control orders.

362. The existing control order regime does not require a person who is required to wear a tracking device to ensure that the tracking device is charged and operational. Requiring a person who is required to wear a tracking device to take steps to ensure that the device is charged and operational is necessary to prevent the effective operation of the requirement from being frustrated 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.

363. New paragraph 104.5(3A)(a) requires the person to take specified steps and reasonable steps to ensure the device is in good working order, while new paragraph 104.5(3A)(b) allows the AFP to take specified steps to ensure the device is in good working order. The phrases “specified steps” and “reasonable steps” are not defined with respect to the new subsection. “Specified steps” will be set out in the control order issued by the issuing authority. “Reasonable steps” will provide a degree of flexibility to allow for appropriate actions to be taken in unforeseen circumstances. This flexibility will ensure that control orders are able to be tailored to the specific circumstances and the specific threat than an individual poses.
364. The phrase “specified steps” in new subsection 104.5(3A) refers to steps set out in the control order that a person must take, or must allow the AFP to take, to ensure a tracking device is kept in good working order. In order to be included in the control order, specified steps must be provided to the issuing court to assist in its determination of whether each is reasonably necessary, and reasonably appropriate and adapted, to one of the purposes set out in paragraph 104.4(1)(d). Examples of specified steps may include a requirement to charge the device for a certain period of time, or that a person allows the AFP to take certain steps after notification that the tracking device is not in good working order.

365. The phrase “reasonable steps” in new subsection 104.5(3A) captures novel situations that require steps to be taken by the person to maintain the tracking device which were not foreseen at the time the control order was sought and subsequently issued. “Reasonable” is to be given its ordinary meaning and will be determined at the time the novel situation arises.

366. New paragraph 104.5(3A)(c) authorises the AFP to enter specified premises to install associated equipment. The provision authorises access to one or more premises as the person the subject of the order may work or reside at multiple locations, where the installation of multiple sets of equipment would make it easier for the person the subject of the order to comply with the conditions of the control order.

367. New paragraph 104.5(3A)(d) requires the person subject to the control order to report 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 at specified times and places to ensure the continued operation of the tracking device.

368. New paragraph 104.5(3A)(e) requires the person subject to the control order to notify the AFP within four hours of becoming aware that the tracking device is 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.
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)**

369. 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.

370. 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

371. 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.

372. Under existing subsection 105.4(5), in order 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).

373. The purpose of the amendments in this Schedule is to clarify how the “imminent” test in subsection 105.4(5) operates. The amendments achieve this by:

- adopting a new defined term of “imminent terrorist act”, and
- clarifying that the thresholds applicable to the AFP member and issuing authority under subsection 105.4(4) apply to the “imminent” test in subsection 105.4(5).

Item 1 – Subsection 105.4(4)

374. This is a consequential amendment. Item 1 replaces all references to “terrorist act” in subsection 105.4(4) with a reference to the new defined term, “imminent terrorist act”. Each reference to “imminent terrorist act” in subsection 105.4(4) should be read to incorporate the complete definition of that term, as outlined in revised subsection 105.4(5). The definition of “imminent terrorist act”, its purpose and intended operation are detailed in item 2.

Item 2 – Subsection 105.4(5)

“Imminent terrorist act”

375. 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.

376. 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.
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. In such circumstances, 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. The current focus of 105.4(5) on the 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.

377. Item 2 amends the “imminent” test in subsection 105.4(5) by adopting a new defined term, “imminent terrorist act”. An “imminent terrorist act” is a terrorist act that:

(i) is capable of being carried out within the next 14 days, and

(ii) could occur within the next 14 days.

378. The defined term seeks to more clearly articulate the underlying policy objective implicit in the original test in subsection 105.4(5).

379. It is important that the test in subsection 105.4(5) clearly includes the ‘capability’ of a person to commit an imminent terrorist act and not just the ‘temporal’ aspect of a planned terrorist act. With the terrorist threat continuing to evolve, radicalisation occurs with increasing speed and terrorists may seek to commit terrorist acts quickly to evade the attention of law enforcement. Law enforcement may be aware that a person has the intention, motivation and necessary tools to commit a terrorist act, but no evidence as to the specific date on which the attack is planned to occur. 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 circumstances, explicit reference to ‘capability’ will ensure that law enforcement is able to take appropriate action to protect public safety and prevent the terrorist act from occurring.

Thresholds

380. 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.

381. 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 and “reasonable grounds to suspect” for an issuing authority.

382. Item 2 clarifies the provisions by clearly articulating that the test of “imminent terrorist act” 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.

**Item 3 – Dictionary in the Criminal Code**

383. Item 3 is a consequential amendment. Item 3 inserts the new defined term “imminent terrorist act” into the Dictionary contained in the Criminal Code.
Schedule 6—Issuing authorities for preventative detention orders

Criminal Code Act 1995

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

384. This item removes the Family Court of Australia or of a State from the definition of “superior court” in section 100.1 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.

385. The primary 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. 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.

386. However, while the other courts within the definition of a “superior court” exercise functions relevant to the areas of criminal law and counter-terrorism, the Family Court does not have jurisdiction in relation to those matters. It is anomalous for a judge of the Family Court to play a role in the control order regime, and no Family Court judge has ever been appointed under section 105.2.

387. This amendment removes the anomaly and means 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 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

388. This item inserts an application provision, “Application provision for certain amendments in the Counter-Terrorism Legislation Amendment Act (No. 1) 2015”, for the amendments to Division 104 of the Criminal Code.

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

390. 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.

391. 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.

392. 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.

393. 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.
394. New subsection 106.7(3) provides that section 105.4 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**

395. 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. 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.

396. The amendments in this Schedule create a “monitoring warrant” regime in a new Part IAAB of the Crimes Act to apply to individuals subject to a control order. 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.

397. 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.**

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

399. 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.

400. 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.

401. 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

402. 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 with confers similar powers conferred by Part IAAB.

3ZZJA Simplified outline of this Part

403. 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.

404. 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

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

406. 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.

407. The expression “damage”, in relation to data, includes damage by erasure of data or addition of other data.

408. 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.

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

410. The expression “issuing officer” means a magistrate.

411. 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.

412. A “monitoring warrant” means a warrant under new section 3ZZOA or 3ZZOB.
413. 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.

414. A “prescribed connection with premises” has the meaning given by new section 3ZZJC.

415. 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.

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

3ZZJC  Prescribed connection with premises

417. Section 3ZZJC outlines the circumstances in which a person has a “prescribed connection” with a premise for the purposes of Part IAAB.

418. 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.

419. 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.

420. 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

421. New section 3ZZJD confirms that certain common law privileges are preserved.
422. 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.

423. 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.

424. 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

425. 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

426. 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

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

428. 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.

429. 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.

430. 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

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

432. 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.

433. 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.

434. 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

435. 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.

436. 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.

437. 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

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

439. 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.
440. 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.

441. 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.

442. 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)).

443. 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

444. 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).

445. 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 is 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).

446. 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.

447. 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 is 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.

448. The first note to subsection 3ZZKE(3) advises readers that the application of new section 3ZZJD means the person’s common law privileges are not abrogated by the 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.

449. Subsection 3ZZKE(4) 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. Subsections 3ZZKE(4) 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.

450. Subsection 3ZZKE(6) 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).

451. 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

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

453. 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.

454. Subsection 3ZZKF(2) authorises a constable to seize evidential material within the meaning of the Crimes Act, other things they have reasonable grounds to believe are evidential material or tainted property within the Proceeds of Crime Act 2002 (POCA), and seizable items. 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 1AA 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.

455. 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

456. 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.

457. 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.
458. 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.

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

460. Subsection 3ZZKG(4) sets out the ways in which 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.

461. 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.

462. 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.

463. 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

464. 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.

465. 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

466. 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

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

468. Subsection 3ZZLC(a) authorises a constable to seize evidential material, 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 and things the constable believes on reasonable grounds to be seizable items. A seizable item is defined in Part 1AA 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

469. 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.

470. 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)).

471. 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

472. 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

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

474. 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.
475. The occupier of the premises can restrict entry by a constable to a particular period and 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)).

476. 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 reasonable practicable after entering the premises (this reflects standard practice).

3ZZNB Consent to search of a person

477. 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.

478. 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.

479. 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

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

481. 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

482. 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

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

3ZZNF Compensation for damage to electronic equipment

484. 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.
Subsection 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. Subsection 3ZZNF(4) sets out matters relevant to the quantum of compensation payable.

3ZZNG  Occupier entitled to be present during search

This section provides the right for the occupier of 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.

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

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

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.

Section 3ZZOA 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.

The matters the issuing officer must have regard to are the nature of the person’s connection with the premises, the matters listed at subsection 3ZZOA(4) including the possibility that the person has engaged, is engaging, or will engage in a terrorist act, or the possibility that the person has contravened, is contravening, or will contravene the control order, and any other matters the issuing officer considers relevant.
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.

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.

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.

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**

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.

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.

The matters the issuing officer must have regard to are the matters listed at subsection 3ZZOB(4) including the possibility that the person has engaged, is engaging, or will engage in a terrorist act, or the possibility that the person has contravened, is contravening, or will contravene the control order, and any other matters the issuing officer considers relevant.

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.

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.

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.
502. 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

503. 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.

504. 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.

505. 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.

506. 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.

507. 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

508. 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.
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.

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.

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.

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.

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**

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.

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**

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.

517. 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

518. 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

519. This section provides that Division 4C of Part IAA of the Crimes Act applies to a thing seized under this 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

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

521. 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

522. 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

523. 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.

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

525. 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

526. 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

527. 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

528. 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 court void.

529. 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 reasonable 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).

530. 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.
Schedule 9—Telecommunications interception

Telecommunications (Interception and Access) Act 1979

Overview

531. 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.

532. 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 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.

533. 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)

534. 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.

Item 2 – Subsection 5(1) (subparagraph (b)(vi) of the definition of permitted purpose)

535. This item clarifies that use of the term “preventative detention order” in the case of the AFP under paragraph 5(1)(b)(vi) has the meaning given in Part 5.3 of the Criminal Code. This is a consequential amendment to items 3 and 4, which insert cross-references to PDOs under state and territory legislation, and repeal the definition of PDO, respectively.

Item 3 – Subsection 5(1) (at the end of paragraph (c) of the definition of permitted purpose)

536. This item amends the definition of “permitted purpose” in section 5(1) of the TIA Act to allow lawfully intercepted information to be used, communicated or recorded in relation to the Commonwealth control order regime and state and territory PDO regimes.
- Division 104 of the *Criminal Code*

- *Terrorism (Police Powers) Act 2002* (NSW)

- *Terrorism (Community Protection) Act 2003* (Vic)

- *Terrorism (Preventative Detention) Act 2005* (Qld)

- *Terrorism (Preventative Detention) Act 2006* (WA)

- *Terrorism (Preventative Detention) Act 2005* (SA)

- *Terrorism (Preventative Detention) Act 2005* (Tas)

- *Terrorism (Extraordinary Temporary Powers) Act 2006* (ACT), and


537. 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.

538. Lawfully intercepted information can already be used, communicated or recorded in relation to the Commonwealth PDO regime. As the preventive detention order 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 PDOs nationally.

**Item 4 – Subsection 5(1) (definition of preventative detention order)**

539. This item repeals the definition of “preventative detention order” in subsection 5(1) of the Act. A definition is no longer required because of the explicit reference to each Commonwealth, state and territory PDO regime, inserted in items 2 and 3.

**Item 5 – Subsection 5(1)**

*Definition of “succeeding control order”*

540. 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 sections 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”*

541. 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.
Items 6 and 7 – Subsection 5B(1)(bc)

542. Item 6 clarifies that use of the term “preventative detention order” in the case of the AFP under paragraph 5B(1)(bc) has the meaning given in Part 5.3 of the Criminal Code.

543. Item 7 amends the definition of “exempt proceedings” in section 5B(1) of the Act to allow state and territory agencies to use lawfully intercepted information in a proceeding relating to the following PDO regimes:

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

544. Lawfully intercepted information can already be used in a proceeding in relation to the Commonwealth PDO regime. As the Commonwealth preventive detention order 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 8 and 9 – Section 6H

545. 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 10 – After section 6S

546. 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.

547. 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.

548. 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 28 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 11 – Subsection 7(9) (note)

549. Item 11 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 12 and 13 – At the end of paragraphs 44A(2)(a) and (b)

550. 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.

Item 14 and 15 – At the end of paragraph 45(2)(a) and (b)

551. 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.

Item 16, 17 and 18 – Section 46

552. 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 19 – At the end of section 46

553. 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.

554. In considering an application for a 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.
555. Before issuing a 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.

556. In addition, the Judge or nominated AAT member must have 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
- 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.

557. 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 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 of the person in question may engage in such conduct or breach the extant control order.

558. 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.

559. 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 20, 21 and 23 – Section 46A

560. 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 22 – After subsection 46A(2)

561. 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.
In considering an application 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.

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
- 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.

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 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 of the person in question may engage in such conduct or breach the extant control order.

565. 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.

Item 24 – At the end of subparagraph 48(3)(d)(ii)

566. 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.

567. 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 the purpose for which the warrant was obtained.

Items 25, 26 and 27 – Section 49

568. 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.
569. Items 25 and 26 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 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 28 – At the end of section 57**

570. 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 section 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 29 – Subsections 63(1) and (2)**

571. 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 53**).

**Items 30, 31 and 32 – Section 65A**

572. These items amend section 65A of the Act which allows 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 no other purpose. This amendment is required to allow an employee of a carrier to communicate information obtained by interception under a warrant relating to a person subject to a control order to an officer of an agency that obtained the warrant.

**Items 33, 34 and 35 – Section 67**

573. These items amend section 67 of the Act to ensure that lawfully intercepted information can be used, communicated or recorded for purposes connected with a control order. Item 35 inserts a new subsection which provides that a “purpose connected with a control order” means:

- a purpose connected with determining whether a control order has been, or is being, complied with, or

- a purpose connected with the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under, Division 104 of the Criminal Code.

**Items 36 and 37 – Sections 79 and 79AA**

574. 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.

575. 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.

576. Subsection 79AA(2) disapplies 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.

577. Item 36 amends the heading to section 79 of the Act in light of the insertion of section 79AA.

**Items 38 and 39 – Section 81A**

578. 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).

579. 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 40 and 41 – Section 81C**

580. 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).

581. 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 42 and 43 – Sections 83 and 85**

582. These items amend sections 83 and 85 of the Act to require the Ombudsman to inspect agencies’ records to ascertain their compliance with new section 79AA. New section 79AA 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**).
Item 44 – At the end of Division 2 of Part 2-8

583. This item inserts a new section 103B, which requires the public reporting of interception warrants relating to a person subject to a control order 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, 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.

584. 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.

585. 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 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.

586. 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.

Item 45 – At the end of subsection 133(2)

587. 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 53).

Items 46, 47, 48, 49 and 50 – New section 139B

588. Item 48 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*
• Division 105 of the Criminal Code
• Terrorism (Police Powers) Act 2002 (NSW)
• Terrorism (Community Protection) Act 2003 (Vic)
• Terrorism (Preventative Detention) Act 2005 (Qld)
• Terrorism (Preventative Detention) Act 2006 (WA)
• Terrorism (Preventative Detention) Act 2005 (SA)
• Terrorism (Preventative Detention) Act 2005 (Tas)
• Terrorism (Extraordinary Temporary Powers) Act 2006 (ACT), and
• Terrorism (Emergency Powers) Act 2003 (NT).

589. 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 51 – Chapter 6 (heading)

590. This item amends the heading to Chapter 6 to “Miscellaneous” because this chapter no longer applies solely to regulations (see Item 53).

Item 52 – Part 6-1 (heading)

591. The heading to Part 6-1 has been amended to “Miscellaneous” because this chapter no longer applies solely to regulations (see Item 53).

Item 53 – Before section 300

592. 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.

593. 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.

594. 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.
595. 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.

596. 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.

**Part 2—Transitional Provisions**

**Item 54 – Validation of dealing with information – preventative detention orders**

597. 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**) would be taken not to have contravened the prohibition on communicating lawfully intercepted information under section 63 of the Act.

598. This validation provision is to 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 Act. This provision is consistent with item 14 of the *Telecommunications (Interception and Access) Amendment Act 2010*, which similarly validated past dealing in lawfully intercepted information in relation to the Commonwealth PDO regime.
Schedule 10—Surveillance devices

Surveillance Devices Act 2004

Overview

599. 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, is 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.

600. 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 device 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 – Subsections 3(aa) and (ab) – Purposes

601. 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

602. 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 clarifies 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

603. Item 3 inserts additional definitions relevant to control orders and PDOs.

604. Under the new definitions the terms ‘confirmed control order’, ‘control order’, ‘engage in a hostile activity’, and ‘interim control order’ take the meanings given in Part 5.3 of the Criminal Code.

605. 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 warrants 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).

606. 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.

607. Items 4 and 5 amend the existing definition of relevant proceeding to include Commonwealth proceedings arising under Divisions 104 (control orders) or 105 (PDOs) of the Criminal Code, or relating to a matter arising under those Divisions (such as an appeal against such an order, a civil suit relating to such an order, or a prosecution relating to such an order). These items also amend the existing definition to include State and Territory proceedings arising under or relating to a matter arising under each jurisdiction’s respective legislation for PDOs. 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.

608. 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

609. 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.
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.

**Items 8 – 18 (Part 2 – Warrants – Division 2 – Surveillance Device Warrants)**

**Application for surveillance device warrant for control orders**

**Item 8 – After subsection 14(3B)**

Item 8 inserts new subsection 14(3B) 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:

(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 9 – Subsection 14(4)**

Item 6 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)**

Subsection 14(6) allows a law enforcement officer to apply for an SD 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:

(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.

Determining the application for a surveillance device warrant for control orders

Item 11 – After paragraph 16(1)(bb)

614. 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.

615. 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:

(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.

616. 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)

617. 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)

618. 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.

619. Item 13 inserts paragraphs 16(2)(eb) and (ec) into subsection 16(2) of the Act. The intention of paragraphs 16(2)(eb) and (ec) 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.

620. 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 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 of the person in question may engage in such conduct or breach the extant control order.

621. 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).

622. 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)**

623. 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)**

624. Subsection 20(2) sets out circumstances in which a chief officer of a law enforcement agency must revoke a surveillance device warrant.

625. 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)**

626. 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.

627. 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.

628. 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.

**Items 19 – 25 (Part 4 – Use of Certain Surveillance Devices Without Warrant)**

**Item 19 – At the end of section 37**

629. 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.

630. 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:

(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 act in a foreign country; or

(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with.

631. 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

632. 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.

633. 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.

634. 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)

635. Item 19 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:

(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 act in a foreign country; or

(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with.

636. 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

637. 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.

638. 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)**

639. 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).

640. 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**

641. 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.

642. 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.

643. 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.

644. 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.

645. 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).

646. 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.
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.

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).

Item 31 amends subsection 45(9) to enable protected information to be used in proceedings arising under, or relating to a matter arising under, state or territory PDO laws. 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

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.

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 – 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.

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)

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. Subsection 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).

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).
655. 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:

(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 act in a foreign country; or

(iv) determining whether a control order has been, or is being, complied with.

656. 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.

**Items 35 and 36 – At the end of subsection 50 and after section 50**

657. Section 50 sets out the requirements for annual reports that are to be provided to the Minister by the chief officer of the law enforcement agency.

658. Items 35 and 36 set out circumstances in which the Minister must defer reporting on specific control order warrants until a subsequent annual report. These arrangements apply only where the Minister is satisfied on the advice of the chief officer of the relevant agency, that contemporaneous reporting could reasonably be expected to enable a reasonable person to conclude that a control order warrant is likely to be in force or not in force in relation to a particular person, object or premises.

659. Subsection 50A(2) provides that if a chief officer is satisfied that information contained in his or her report under subsection 50(1), if made public, could reasonably be expected to enable a reasonable person to conclude that a control order warrant relating to a particular premises, person or object is likely to be, or not to be, subject to a control order, he or she must advise the Minister to exclude the information from the report before causing the report to be laid before Parliament.

660. Subsections 50A(3) provides that if the Minister is satisfied, on the advice of the chief officer, that the information, if made public, a person could reasonably be expected to make this conclusion, then the Minister must exclude it from the report.

661. The new subsections 50A(2) and (3) recognise risks in publicly reporting on the use of surveillance devices in the context of control orders. It is common for only very limited numbers of control orders to be in force at any given time. Persons subject to control orders are aware of the order. Accordingly, reporting on the number of control order warrants that are in force would likely allow the person subject to a control order and others to extrapolate with some certainty whether a control order warrant is or is not in effect. This risk would be exacerbated if a particular control order contains a particular limitation or restriction that would be particularly amenable to monitoring by way of a surveillance device.

662. If a person knows, or can reasonably speculate with some certainty, that there is a control order warrant in place, they are more likely to be able to modify their behaviour to defeat those lawful surveillance efforts. Comparatively, if a person knows, or can reasonably speculate with some certainty, that a control warrant is not in force, the specific deterrence
value of the control order is likely to be diminished to the extent that the person believes they can engage in proscribed activity without risk of detection.

663. New subsections 50A(4) and (5), however, require that information previously excluded under new subsections 50A(2) and (3) from a report be made available in subsequent reports. This ensures that the key requirements of accountability and transparency retained, albeit in a delayed manner. In practice, reporting will always be required in the report following the expiry of all control orders relating to a person, and possibly sooner (if there are many control orders in force).

664. Subsection 50A(4) requires that, if the chief officer is satisfied that the information that was excluded from a previous annual report, if now made public, could not reasonably be expected to enable a reasonable person to conclude that a control order warrant is in place is in place regarding a control order that is in force, then they must advise the Minister to include it in the next report in accordance with subsection 50(1) of the Act.

665. Subsection 50A(5) requires that, if the Minister is satisfied, on the advice of the chief officer, that the information, if made public, could not reasonably be expected to enable a reasonable person to conclude that a control order warrant is in place is in place regarding a control order that is in force, then this information should be include in the next report in accordance with subsection 50(1).

666. All information, despite not being reported in a particular annual report tabled in the Parliament, must still be reported to the Minister in accordance with sections 49 and 50.

667. Importantly, if there is a lapse of time between subsections 50A(2) and 50A(3) or between 50A(4) and 50A(5), and circumstances change, it may be the case that the Minister may not be satisfied on the basis of a chief officer’s advice that excluding these details from the report is necessary. For example, if a control order is in force in relation to a person shortly after the end of a financial year, when the chief officer of a law enforcement agency submits his or her annual report to the Minister, but is no longer in force at the point in time at which the Minister is considering tabling his or her report in Parliament, the Minister may conclude that any risks identified by the chief officer no longer exist.

Item 37 – At the end of paragraph 52(1)(j)

668. Section 52 lists records that the chief officer of a law enforcement agency is required to ensure are kept. Item 37 inserts 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 38 – After subparagraph 53(2)(c)(iiib)

669. 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.

670. Item 38 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 39 – Part 7 – Miscellaneous

After section 65 – Sections 65A and 65B

Section 65A

671. 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.

672. 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:

a. protect persons from criminal liability for acts done, or omitted to be done, otherwise than in good faith

b. 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

c. protect law enforcement agencies from civil liability in these circumstances.

Section 65B

673. New section 65B permits the use of information obtained under a control order warrant. The intention 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. Preventative detention orders can typically only be obtained where the issuing authority is satisfied inter alia that making the order would substantially assist in preventing a terrorist act occurring.

674. Paragraph 65B(1)(a) provides the scope in which this section applies, and requires that one of four conditions be satisfied: that a control order warrant was issued on the basis that an interim control order was in force; a tracking device was issued on the basis that an interim control order was in force; an optical surveillance device was used under subsection 37(4) on the basis that an interim control order was in force; or a surveillance device was used under subsections 38(3A) or (6) on the basis that an interim control order was in force.

675. Paragraphs 65B(1)(b) to (f) set out the respective qualifying conditions in paragraph 65B(1)(a) only apply if the purported exercise of a power, or the purported performance of a function or duty, in the case of that purported exercise of a power, is consequential on a control order warrant, tracking device authorisation, or use of a
surveillance device without warrant as permitted by subsections 37(4), 38(3A) or 38(6) of the Act.

676. Subsection 65B(2) permits using, communicating or publishing the information obtained, 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 to a person, or serious damage to property, or for a purpose connected with a PDO.

677. Subsection 65B(3) permits the information to be admitted in evidence in any proceedings if doing so is necessary to assist in preventing or reducing the risk of the commission of a terrorist act, serious harm to a person, or serious damage to property, or if the information is admitted for a purpose connected with a PDO (such as part of an application for a PDO, or a subsequent appeal against such an order).

678. Subsection 65B(3) does not permit the use of protected information in proceedings confined to the determination of whether a person subject to a control order has complied, or is complying, with the control order responsibilities, conditions and prohibitions.

679. Subsection 65B(5) inserts a definition that gives “serious harm” the meaning given in the Criminal Code.
Schedule 11—Offence of advocating genocide

Criminal Code Act 1995

Overview

680. 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.

681. The amendments in this Schedule create a new offence of publicly 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. It only applies to advocacy done publicly.

Item 1 – Part 5.1 of the Criminal Code (heading)

682. 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)

683. 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)

684. 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

685. This item inserts new section 80.2D providing the new “Advocating genocide” offence at the end of Subdivision C of Division 80.

686. New subsection 80.2D(1) creates a new offence for publicly advocating genocide. While “publicly” is not defined, it would include, but not be limited to:

- causing words, sounds, images of writing to be communicated to the public, a section of the public, or a member of members of the public
- conduct undertaken in a public place, or
- conduct undertaken in the sight or hearing of people who are in a public place.

687. 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 publicly 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.

688. 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. 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, along with the offence prohibiting
advocating terrorism, which came into effect on 1 December 2014, is intended to be one of
those tools.

689. 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.

690. 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.

691. New subsection 80.2D(2) “double jeopardy” provides that a person cannot be tried for
the offence of advocating genocide in an Australian court if the person has already been
convicted or acquitted by the International Criminal Court in relation to that conduct.

692. New subsection 80.2D(3), “Definitions” provides that, for the purposes of the offence
in subsection 80.2D(1), “advocates” as counselling, promoting, encouraging or urging the
commission of a genocide offence. Those expressions will have their ordinary meaning. The
terms “promotes” and “encourages” 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 of 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.

693. 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 that a
government policy is mistaken, contains an error, or is defective in good faith, are 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 somebody would take that speech as advocating the commission of a genocide offence.

694. 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).

695. 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.

696. 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

697. 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.

698. 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.

699. 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.

Technical and consequential amendments (items 1, 2, 3 and 7)

700. 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.

701. 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)

702. This item repeals and replaces existing subsection 40(1) and paragraphs 40(1)(a) and 40(1)(b).

703. 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.

704. 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”.

111
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).

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 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 inter-governmental 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)

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.

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. The accountability mechanisms already provided for in the ASIO Act in relation to rights of notice and review when ASIO furnishes a security assessment will not be altered.

Item 6 – Subsection 40(3)

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 8 – Subsection 65(1)(b)

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 9-13)

711. The amendments to section 40 of the ASIO Act will require consequential amendments to 29B, 39A(2), (6), (7), (8) and (12), 39A(15)(b), 39A(15) and 43AAA(4) and 5 of the AAT Act 1975 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). Item 9-13 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.

712. For example, item 9 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.


Item 1 – Paragraph 9A(2)(a)

713. 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.

714. 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.

715. 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.

716. 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.

717. 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.

718. 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”.

Item 2 – Application

719. 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

720. The purpose of these amendments is to clarify the threshold requirements for the issue of a delayed notification search warrant. The amendments clarify that, while an eligible officer applying for a delayed notification search warrant 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.

721. These amendments do not make any substantive change to the requirements for obtaining a delayed notification search warrant. 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 simply to clarify that neither a chief officer nor an eligible issuing officer is 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 delayed notification search warrant and are not in a position to personally suspect or believe the relevant matters.

**Item 1 – Section 3ZZAC (definition of conditions for issue)**

722. Item 1 repeals the definition of “conditions for issue” in section 3ZZAC. This amendment is consequential to a range of other amendments to the delayed notification search warrant regime.

**Item 2 – Section 3ZZBA**

723. This item repeals existing section 3ZZBA, removing the “conditions for issue” in relation to the issue of a delayed notification search warrant, 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 delayed notification search warrant.

724. 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 beliefs – currently referred to as the “conditions for issue”.

725. 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 delayed notification search warrant.

726. 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.

727. 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.

728. 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 delayed notification search warrant. 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)

729. 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 delayed notification search warrant.

730. New subsection 3ZZBB(1A) provides that, where an eligible officer seeks the chief officer’s authorisation to apply for a delayed notification search warrant in relation to particular premises, the conditions in section 3ZZBB must be met.

731. New subsection 3ZZBB(1) provides that, before authorising an eligible officer to apply for a delayed notification search warrant, 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.

732. 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 delayed notification search warrant would frustrate the effectiveness of executing the warrant.

Item 4 – Subsection 3ZZBC(1) (paragraph (a) of note 1)

733. Item 4 amends note 1 to subsection 3ZZBC(1), which sets out the factors to be addressed in an application for a delayed notification search warrant. 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.
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)**

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 delayed notification search warrant.

This amendment clarifies that the eligible issuing officer is not required to personally hold the relevant suspicion or belief before issuing a delayed notification search warrant. 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)**

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 delayed notification search warrant 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)**

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)**

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)**

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)**

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)

742. 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.

743. 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)

744. 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

745. This item confirms that the present amendments have no effect on the validity of a delayed notification search warrant issued, or an authorisation or application made, before these amendments commenced.
Schedule 15—Protecting national security information in control order proceedings

National Security Information (Criminal and Civil Proceedings) Act 2004

Overview

746. 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).

747. The NSI Act provides a range of protections for sensitive information, the disclosure of which is likely to prejudice national security. These options include the ability to allow sensitive information to be redacted, and prevent a witness from being required to give evidence.

748. 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.

749. 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.

750. 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.

Procedural requirements for control orders

751. Control orders require a detailed application to be prepared and presented to an issuing court.

752. 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.

753. 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.

754. 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 1995 (section 104.28A(2)).

755. 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**

756. 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**

757. 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. 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.

758. Following the closed court 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)).

759. 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.

760. 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**

761. 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)).

762. The amendments provide that where a closed hearing is held under section 38I 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 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

763. The new orders will only be available in proceedings relating to making, confirming or varying a control order under Division 104 of the Criminal Code.

Presence in the closed court hearing under section 38I

764. The amendments 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 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 proceedings. 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.

Prerequisite for granting an order under new subsection 38J

765. 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) still has been given sufficient notice of the allegations on which the control order request was based, even if the individual may be denied notice of the information supporting those allegations. This ensures that the subject (or proposed 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.

766. 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 section 38J

767. 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 section 38J would have a substantial adverse effect on the substantive hearing in the proceeding, and
- any other matter the court considers relevant.

768. 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)

769. 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.

770. 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 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)

771. 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.

772. 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)

773. 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.

774. 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)

775. 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)

776. 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)

777. 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 a closed 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)

778. 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.

Item 8 – Paragraphs 38H(5)(b), (6)(a) and (6)(b)

779. 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.
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 a 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.

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 a 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)

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.

Item 10 – Subsection 38I(1)

Item 10 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).

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). 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 19).

Item 11 – Subsection 38I(1) (note)

Item 11 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 12 – After subsection 38I

Item 12 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 closed hearing under section 38I that is held to determine if or 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.

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 closed 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).

**Item 13 – Paragraph 38I(5)(a)**

788. Item 13 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 14 – Subsection 38I(6)**

789. Item 14 corrects an error in subsection 38I(6) by removing a reference to section 38K which no longer exists in the NSI Act.

**Item 15 – Paragraph 39I(9)(a)**

790. 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 closed 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.

791. Item 15 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 a court has made an order under new subsection 38I(3A) that the party and their legal representative are not entitled to be present during any part of the closed hearing.

**Item 16 – Subparagraph 38I(9)(a)(i)**

792. Item 16 is a minor consequential drafting amendment as a result of item 15. It does not change the effect of the provision.

**Item 17 – Subparagraph 38I(9)(a)(iii)**

793. Item 17 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 19 and replaced with new section 38J. The content of former section 38J is in new subsection 38I(10) (see item 18).

**Item 18 – At the end of section 38I**

794. Item 18 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 19 – Section 38J**

795. Item 19 repeals and substitutes existing section 38J (the contents of which has been relocated to new subsection 38I(10)).

796. 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.

797. 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 notice of the allegations on which the control order request was based, even if the relevant person may be denied notice of the information supporting 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 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.

798. 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.

799. 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. Under new subsection 38I(3A) the court may exclude the relevant person and their legal representative from hearing the information, even if they have an appropriate security clearance.
800. New paragraph 38J(2)(e) 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.

801. 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 the latter order, 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. Under new subsection 38J(3), the court order would not provide for a copy of the document with the national security information deleted, or a copy of the document with the information deleted and either a summary of the deleted information or a statement of facts that the deleted information would or would be likely to prove. When this information is disclosed to the court, the closed hearing requirements under section 38I will apply.

802. 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.

803. 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.

804. 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.

805. 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 20 – Subsection 38L(1)**

806. Item 20 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 21 – At the end of subsection 38L(1) (note)

807. Item 21 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 22 – At the end of subsection 38L(6)

808. Item 22 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).

809. Item 22 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 23 – Subsection 38M(1)

810. Item 23 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 24 – Subsections 38P(1) and (2)

811. Item 24 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 25 – Section 38R

812. Item 25 amends the heading of section 38R to provide, in accordance with the amendment in item 26, that the same appeal rights in respect of orders made under section 38L apply in respect of orders made under revised section 38J.

Item 26 – Subsection 38R(1)

813. Item 26 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 27 – Application of amendments

814. Item 27 relates to the application of the amendments contained in this Schedule. Item 27 provides that the amendments under this Schedule apply to a civil proceeding that begins before or after the commencement of this Schedule. Accordingly, these amendments 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 28 – Section 8 (paragraph (f) of the definition of designated publication restriction)

815. Item 28 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.
Schedule 16—Dealing with national security information in proceedings

National Security Information (Criminal and Civil Proceedings) Act 2004

816. 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.

817. 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)

818. 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

819. This Schedule amends section 19 to allow the court to make an order enabling the parties and the Attorney-General to agree to depart from the NSI Regulation in relation to particular national security information.

Orders made under subsections 22(2) or 38B(2)

820. 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

821. 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)

822. 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)

823. This item inserts paragraph 19(1B) which provides that paragraph (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)

824. 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)

825. This item inserts paragraph 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)

826. This item repeals subsection 23(2) and in substitution provides that the matters described in paragraph (1)(a) or (b) of section 23 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)

827. This item repeals subsection 38(C)(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**

828. 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.

829. 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.

830. 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)

831. This item inserts a new item in subsection 355-65(2) of Schedule 1 of the TAA.

832. Section 355-25 of the TAA 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, sets out the exceptions to the offence provision for disclosures relating to social welfare, health or safety.

833. The amendment will create an additional exception to the offence provision, authorising taxation officers to disclose information to an Australian government agency for the listed purposes. The purposes are limited to preventing, detecting, disrupting or investigating conduct that relates to a matter of security as defined by section 4 of the ASIO Act.

834. Security as defined in the ASIO Act means:

- 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
- the protection of Australia's territorial and border integrity from serious threats; and
- 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).

835. 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.

836. With the increased tempo of counter-terrorism operations, it is sometimes necessary for Australian government agencies with national security functions to intervene early in a person’s engagement in terrorist activities to protect community safety.

837. Subsection 355-70 of Schedule 1 of the TAA sets out the exceptions to the offence provision for disclosures relating to law enforcement and related purposes. The amendment is separate and distinct from the existing subsection 355-70 item 1 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. In contrast, the amendment seeks to allow disclosure to multi-jurisdictional agencies such as the National Distribution Group, which coordinates joint Commonwealth and State and Territory agency capabilities to prevent,
disrupt and prosecute terrorism related activities. Consequently, disruption in this sense comprises a range of activities beyond traditional law enforcement.

838. The amendment will further allow disclosure for listed purposes to other Australian government agencies, with national security functions, such as the National Distribution Group, that may not currently be in existence. The amendment is drafted to ensure 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 by that Group at short notice, will be covered by the exception.

839. A taxation officer will only be authorised to disclose the requested 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.

840. 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 – Application**

841. This item provides that the amendment of the TAA in Item 1 applies in relation to records and disclosures of information made on or after the commencement of this Schedule, whether the information was obtained before, on or after that commencement.