THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

TELECOMMUNICATIONS LEGISLATION AMENDMENT (INTERNATIONAL PRODUCTION ORDERS) BILL 2020

EXPLANATORY MEMORANDUM

(Circulated by authority of the Minister for Home Affairs, the Hon Peter Dutton MP)
GENERAL OUTLINE

1. The Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill) will amend the Telecommunications (Interception and Access) Act 1979 to establish a new framework to assist Australia’s international crime cooperation efforts by improving Australian agencies’ access to overseas communications data for law enforcement and national security purposes.

2. Almost every crime type and national security concern has an online element—agencies require electronic information and communications data not only for cyber investigations but also for investigations and prosecutions regarding violent crimes, human trafficking and people smuggling, drug trafficking, financial crimes, terrorism and child sexual abuse.

3. The exponential rise of global connectivity and reliance on cloud computing means that intelligence and evidence that was once stored within Australia and available under a domestic warrant or authorisation is now distributed over different services, providers, locations and jurisdictions, and is often only obtainable through international cooperation.

4. Criminals, including terrorists, typically access communications services that are supplied or operated by entities outside Australia. The overwhelming majority of data from these services is held by companies located overseas, including the United States. This places these service providers in a unique position to assist Australian law enforcement and national security efforts.

5. The extensive use of foreign telecommunications and online platforms by both criminals and terrorists has made accessing this data increasingly valuable. Australian law enforcement and national security agencies require timely access to electronic information and communications data from foreign communications providers for criminal investigations and prosecutions, as well as other law enforcement and national security purposes. To collect this data, Australia has relied heavily on mutual legal assistance from overseas jurisdictions, particularly the United States, where many communications providers of interest are located. Accessing communications data through the mutual legal assistance regime is a lengthy process, which cannot keep pace with the fast moving requirements of the investigation and prosecution of serious crime.

6. To address this issue, Australia is seeking to negotiate agreements with like-minded foreign governments for reciprocal cross-border access to communications data. It is anticipated that these agreements would allow law enforcement and national security agencies in each participating country to issue orders, through a competent authority, for the production of data directed to communications and technology companies in the other country’s jurisdiction. These agreements would significantly reduce the time it currently takes to acquire communications data that is vital to law enforcement and security efforts.

7. The Bill provides the legislative framework for Australia to give effect to future bilateral and multilateral agreements for cross-border access to electronic information and communications data.
8. **Schedule 1** of the Bill will:

- introduce a regime for Australian agencies to obtain independently-authorised international production orders for interception, stored communications and telecommunications data directly to designated communications providers in foreign countries with which Australia has a designated international agreement;

- provide that international production orders:
  - may be sought by agencies permitted under the *Telecommunications (Interception and Access) Act 1979* to seek warrants for domestic interception or stored communications or authorisations for access to telecommunications data; and
  - may be sought by law enforcement agencies for the purposes of investigating a serious criminal offence or monitoring a person subject to a control order; and
  - may be sought by the Australian Security Intelligence Organisation for the purpose of it carrying out its functions;

- establish an Australian Designated Authority to review international production orders for compliance with the nominated designated international agreement and act as an intermediary between Australian law enforcement and national security agencies and designated communications providers, including giving international production orders to designated communications providers and, in some cases, receiving data back from designated communications providers pursuant to international production orders;

- include provisions relating to other aspects of the new international production order regime, such as:
  - application, issuing, giving and revocation procedures;
  - requirements to be met for an order to be able to be issued;
  - compliance with orders;
  - oversight, reporting and record-keeping;
  - disclosure of protected information; and
  - evidentiary certificates;

- clarify the interaction between the new regime and the requirements of the *Telecommunications Act 1997, Telecommunications (Interception and Access) Act 1979* and *Privacy Act 1988*, to ensure that Australian communications providers are not prevented from responding to incoming orders and requests for electronic information and communications data from foreign countries with which Australia has a designated international agreement. The Schedule does not place any obligations on Australian communications providers under Australian law to respond to incoming requests for information from foreign countries.
- establish an appropriate enforcement mechanism with civil penalties. Designated communications providers will be required to comply with international production orders to the extent they are capable of doing so, and subject to the provider meeting a particular enforcement threshold.

- make consequential amendments to the *Freedom of Information Act 1982*, *International Criminal Court Act 2002*, *Law Enforcement Integrity Commissioner Act 2006* and *Mutual Assistance in Criminal Matters Act 1987*, to ensure that information obtained by Australian agencies pursuant to an international production order is subject to appropriate protections and permitted uses, consistent with the treatment of information obtained under a domestic warrant or authorisation.

**ABBREVIATIONS**

The following abbreviations will be incorporated throughout this explanatory memorandum:

- Administrative Appeals Tribunal (AAT)
- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Security Intelligence Organisation (the Organisation)
- Inspector-General of Intelligence and Security (IGIS)
- *International Covenant on Civil and Political Rights* (ICCPR)
- International Production Order (IPO)
- Public Interest Monitors (PIMs)
- *Telecommunications (Interception and Access) Act 1979* (TIA Act)
- Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill)

**FINANCIAL IMPACT**

9. Nil, as financial impacts will be met from existing appropriations.
STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

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

Telecommunications Legislation Amendment (International Production Orders) Bill 2020

1. 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

2. The Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill) will amend the Telecommunications (Interception and Access) Act 1979 (TIA Act) to enhance the process of exchanging information held by designated communications providers for the purpose of criminal investigations and prosecutions.

3. The Bill introduces three International Production Orders (IPOs) to allow Commonwealth, state and territory law enforcement and national security agencies to more efficiently acquire data held in a foreign country by a designated communications provider.

Human rights implications

4. The human rights and freedoms engaged by the Bill fall under the following Articles of the International Covenant on Civil and Political Rights (ICCPR) to which Australia is a State Party:

   - protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR
   - protection of the right to freedom of expression contained in Article 19 of the ICCPR
   - the right to life contained in Article 6 of the ICCPR, and
   - the right to effective remedy contained in Article 2(3) of the ICCPR.

Schedule 1

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

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

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

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

8. The provisions that will enable Commonwealth, state and territory law enforcement and national security agencies to seek data from communications providers engage the protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR. This is for two reasons: firstly, the Bill introduces a regime where – subject to an agreement – foreign communications providers may facilitate Australian law enforcement and national security agencies’ access to private communications data where an underlying IPO is present. Secondly, the Bill enables Australian communications providers to facilitate the government of a foreign country’s access to private communications data, where an appropriate order is in place.

*International Production Orders - interception*

9. Provisions in Schedule 1 of the TIA Act will allow *interception agencies*, *control order IPO agencies*, and the Australian Security Intelligence Organisation (the Organisation) to apply for an IPO directing a *designated communications provider* to provide communications carried by the individual carriage service during a specified period.

*Interception agencies and control order IPO agencies*

10. An *interception agency* includes, among others, the Australian Federal Police (AFP), Australian Commission for Law Enforcement Integrity, the Australian Criminal Intelligence Commission (ACIC), and authorised state and territory police forces. *Control order IPO agency* includes the AFP, the ACLEI, the ACIC, and designated state authorities under section 34 of the TIA Act.

11. Only an eligible judge or nominated Administrative Appeals Tribunal (AAT) member may issue an IPO relating to interception as a result of an application made by an *interception agency* or a *control order IPO agency*. Having authorised members of the AAT being able to issue IPOs in addition to an eligible judge is consistent with the existing framework under the TIA Act.

12. The eligible judge or nominated AAT member (together referred to as ‘the decision maker’) may only issue an IPO relating to interception where they are satisfied on reasonable grounds a particular person is using or is likely to use the communications service, and the extent to which information gathered under the order would be likely to assist the detection, prevention, investigation or prosecution of an offence which either carries a maximum penalty of at least 7 years imprisonment or life imprisonment, or is a serious offence under

---

section 5D of the TIA Act. Under section 5D, serious offences are offences of certain specified categories including murder, kidnapping and terrorism, offences that carry a maximum term of imprisonment of 7 years, and a series of listed specified other offences.

13. The decision maker may only issue an IPO in relation to interception activities for a period no longer than 90 days for interception agencies and control order IPO agencies.

14. In deciding whether to issue an IPO relating to interception, the decision maker must have regard to several matters including relevantly, how much the privacy of any person or persons would be likely to be interfered with. The decision maker must also take into account the availability and use of other means to achieve the objectives of the IPO, including how much the use of such methods would assist with or be likely to prejudice the investigation (e.g. by delay).

15. This means that where there are other methods to access the necessary information that would be less intrusive on the privacy of the person, the relevant agency may be required to turn to those means instead of seeking an IPO for interception activities.

16. In addition, there are other considerations the decision maker must take into account, which vary according to the order being sought. Broadly, the decision maker must consider the gravity of the conduct concerned, and to what degree the order will assist in the detection, prevention, investigation or prosecution of the offence. There are other, more specific considerations; for example, for an IPO relating to control orders, the decision maker must also take into account the likelihood that a person will breach a control order. Each of these factors go toward ensuring that actions taken under the IPO, including the necessary interference with a person’s privacy, are proportionate to the relevant conduct.

17. Specifically in relation to IPOs relating to control orders, the Bill includes an additional privacy consideration that orders in relation to the enforcement of criminal law or national security do not possess. For IPOs relating to control orders, the decision maker must consider whether intercepting communications would be the method that is likely to have the least interference with any person’s privacy. This additional requirement was inserted into the Bill (and forms part of the current domestic control order warrant regime) on the basis that additional protection is considered appropriate noting the IPO can be issued for purposes in connection with the monitoring of a person subject to a control order rather than in connection with an investigation into a specific serious offence.

The Organisation

18. Prior to the Organisation applying for an IPO, the consent of the Attorney-General must be obtained in writing, except in urgent circumstances where it may be obtained verbally. Once the Attorney-General’s consent is obtained, the Organisation may then apply to a nominated AAT Security Division member for an IPO.

19. The nominated AAT Security Division member may only issue an IPO relating to interception where they are satisfied on reasonable grounds a particular person is using or is likely to use the communications service, and the extent to which information gathered under the order would be likely to assist the Organisation in carrying out its functions in relation to security.
20. The nominated AAT Security Division member may issue an IPO in response to an application made by the Organisation for a period no longer than 6 months.

21. In deciding whether to issue an IPO relating to interception, the nominated AAT Security Division member must have regard to whether other less intrusive means of obtaining intelligence relating to security are available, or have been used. The less intrusive method is then weighed against its effectiveness and potential to prejudice the Organisation in carrying out its functions (e.g. by delay).

22. This means that where there are other methods to access the necessary information that would be less intrusive on the privacy of the person, the Organisation may be required to turn to those means instead of seeking an IPO for interception activities. While an application by the Organisation does not need to be assessed with respect to other privacy considerations, the Organisation must conduct their security intelligence activities in accordance with Ministerial Guidelines. This includes, among other things, that the Organisation’s actions should be proportionate to the gravity of the threat posed and the probability of its occurrence, and that inquiries and investigations should be done with as little intrusion into privacy as possible.

Summary

23. As a result, the Bill provides the decision maker or nominated AAT Security Division member must evaluate the individual circumstances of each application made by interception agencies, control order IPO agencies, and the Organisation. They must turn their mind to the interests of the agency applying for an IPO, as well as wider public interests, such as the impact on privacy. To assist the decision maker or nominated AAT Security Division member reach a decision in connection with an application, they have the discretion to seek additional information from the relevant agency to further inform their assessment of the application.

24. Therefore, the amendments do not constitute an arbitrary or unlawful incursion into the protection against arbitrary or unlawful interference with a person’s privacy. To the extent that there is a limitation on the protection against arbitrary or unlawful interference with privacy, statutory safeguards ensure any interference is reasonable, necessary and proportionate.

Public Interest Monitors

25. Public Interest Monitors (PIMs) currently operate in Victoria and Queensland. They were established under the Public Interest Monitor Act 2011 (Vic), the Police Powers and Responsibilities Act 2000 (Qld), and the Crime and Corruption Act 2001 (Qld). The PIM provides safeguards in relation to applications by Victorian and Queensland law enforcement agencies for various warrants, orders or approvals to use certain covert or coercive investigative powers, by:

- appearing at hearings of applications to test the content and sufficiency of information relied upon;
- questioning any person giving information in relation to the application; and
- making submissions as to the appropriateness of granting the application.
26. Parts 2 and 3 of Schedule 1 of the TIA Act include provisions that allow the intervention of the Victorian and Queensland PIMs to assess the applications for interception activities made by their jurisdiction’s relevant agency.

27. To enable the PIMs to provide effective oversight, provisions in the Bill permit the PIMs to have access to the necessary information relevant to the agency’s application for an IPO for interception, including the power to question relevant persons supporting the application for an order.

28. Based on the information before them, the PIMs may make an assessment of the application against the same criteria that the decision maker will use to make their assessment. The PIMs may submit their assessment to the decision maker which then must be considered in the decision maker’s assessment of the application.

29. Victorian and Queensland PIMs will add an additional layer of oversight to ensure the use of the IPO framework by agencies in their jurisdictions is appropriate and remains consistent with their use of the current domestic warrant regime under the TIA Act.

30. For these reasons, the inclusion of provisions relevant to PIMs strengthens the existing protections in the Bill against arbitrary or unlawful interference with privacy in Victoria and Queensland. Moreover, while the current provisions relating to PIMs are relevant only to Victoria and Queensland, there is scope to accommodate similar oversight bodies in the framework, should they be established in other jurisdictions in the future.

**B-Party interception**

31. Several provisions in the Bill enable B-Party services to be the subject of an IPO in relation to interception activities in limited and controlled circumstances. B-Party interception activities involve the interception of a communications service of a person who is not a person involved in an investigation of a relevant offence (the B-Party).

**Interception agencies and control order IPO agencies**

32. For applications made by interception agencies and control order IPO agencies, the decision maker must have reasonable grounds for suspecting the person involved in the offence is likely to communicate using the particular communications service of the B-Party. In deciding whether to issue a B-Party order relating to interception, the decision maker must have regard to several matters including relevantly, how much the privacy of any person or persons would be likely to be interfered with. The decision maker must also take into account the availability and use of other means to achieve the objectives of the IPO, including how much the use of such methods would assist with or be likely to prejudice the investigation (e.g. by delay).

33. This means that where there are other means to access the necessary information that would be less intrusive on the privacy of the person, the relevant agency may be required to turn to those means instead of seeking an IPO seeking interception activities.

34. In addition, there are other considerations the decision maker must take into account, which vary according to whether the order is being sought by an interception agency or a control order IPO agency. Broadly, the decision maker must consider the gravity of the conduct concerned, and how much the order will assist in the detection, prevention,
investigation or prosecution of the offence. Each of these factors go toward ensuring that actions taken under the IPO, including the necessary interference with a person’s privacy, are proportionate to the relevant offence.

The Organisation

35. Applications for B-Party interception made by the Organisation must satisfy the nominated AAT Security Division member there are reasonable grounds for suspecting the person involved in the offence is likely to communicate using the particular communications service of the B-Party. In deciding whether to issue a B-Party order relating to interception, the nominated AAT Security Division member must have regard to whether other less intrusive means of obtaining intelligence relating to security are available, or have been used. The less intrusive method is then weighed against its effectiveness and potential to prejudice the Organisation in carrying out its functions (e.g. by delay).

36. This means that where there are other means to access the necessary information that would be less intrusive on the privacy of the person, the Organisation may be required to turn to those means instead of seeking an IPO seeking interception activities. While an application by the Organisation does not need to be assessed with respect to other privacy considerations, the Organisation must conduct their security intelligence activities in accordance with Ministerial Guidelines. This includes, among other things, that the Organisation’s actions should be proportionate to the gravity of the threat posed and the probability of its occurrence, and that inquiries and investigations should be done with as little intrusion into privacy as possible.

Restrictions on issuing order

37. Of chief importance, a decision maker or nominated AAT Security Division member is restricted from issuing an IPO seeking B-Party interception unless they are satisfied the relevant agency has exhausted all other practicable methods of identifying the telecommunications services used by the person involved in the offence, or it is not otherwise possible to intercept the telecommunications used by the person involved in the offence.

38. B-Party interception IPOs must not be longer than 45 days for interception agencies and control order IPO agencies. The Organisation may use B-Party interception for up to 3 months. These periods are half that applicable to a non B-Party telecommunications interception warrant, as B-Party interception inherently involves a potential for greater privacy intrusion of persons who may not be involved in the commission of an offence.

39. Under this formulation, B-Party IPOs for interception activities are a means of last resort. The restrictions on the circumstances for when an order may be issued and the duration of time for which an order remains in force appropriately balances the desire to protect the privacy of individuals not the subject of investigation against the need for effective law enforcement and national security.

40. The provisions enabling the issuance of B-Party IPOs are therefore a proportionate and necessary limitation on the protection against arbitrary or unlawful interference with privacy under Article 17 of the ICCPR.
International Production Orders - stored communications and telecommunications data

41. The provisions in Schedule 1 of the TIA Act will allow criminal law-enforcement agencies, control order IPO agencies, and the Organisation to apply for an IPO directing a designated communications provider to obtain stored communications.

42. A criminal law-enforcement agency captures the same definition as the existing framework under the TIA Act and includes, among others, the AFP, the ACLEI, the ACIC, and state and territory police forces.

43. An enforcement agency, control order IPO agency, and the Organisation may also apply for an IPO directing a designated communications provider to obtain telecommunications data for a specific period. An enforcement agency has the same meaning as in the TIA Act.

Enforcement agencies and control order IPO agencies

44. Only an issuing authority may issue an IPO relating to stored communications or telecommunications data as a result of an application made by a criminal law-enforcement agency, enforcement agency, or control order IPO agency.

45. The issuing authority or nominated AAT Security Division member (together referred to as ‘the decision maker’) may only issue an IPO relating to stored communications or telecommunications data where they are satisfied on reasonable grounds a particular person is using or is likely to use the individual carriage service, and the extent to which information gathered under the order would be likely to assist the detection, prevention, investigation or prosecution of an offence which carries a maximum penalty of at least 3 years imprisonment or life imprisonment.

46. In deciding whether to issue an IPO relating to stored communications or telecommunications data, the decision maker must have regard to several matters including relevantly, how much the privacy of any person or persons would be likely to be interfered with. The decision maker must also take into account the availability and use of other means to achieve the objectives of the IPO, including how much the use of such methods would assist with or be likely to prejudice the investigation (e.g. by delay).

47. In addition, there are other considerations the decision maker must take into account, which vary according to which order is being sought. Broadly, the decision maker must consider the gravity of the conduct concerned, and how much the order will assist in the detection, prevention, investigation or prosecution of the offence. Each of these factors go toward ensuring that actions taken under the IPO, including the necessary interference with a person’s privacy, are proportionate to the relevant conduct.

The Organisation

48. Prior to the Organisation applying for an IPO relating to stored communications the consent of the Attorney-General must be obtained in writing, except in urgent circumstances where it may be obtained verbally. Once the Attorney-General’s consent is obtained, the Organisation may then apply to a nominated AAT Security Division member for an IPO. The consent of the Attorney-General is not required where the Organisation applies for an IPO.
seeking *telecommunications data*. This is consistent with current arrangements in the TIA Act.

49. In deciding whether to issue an IPO relating to stored communications or *telecommunications data*, the nominated AAT Security Division member must have regard to whether other less intrusive means of obtaining intelligence relating to security are available, or have been used. The less intrusive method is then weighed against its effectiveness and potential to prejudice the Organisation in carrying out its functions (e.g. by delay).

50. This means that where there are other methods to access the necessary information that would be less intrusive on the privacy of the person, the Organisation may be required to turn to those means instead of seeking an IPO for interception activities. While an application by the Organisation does not need to be assessed with respect to other privacy considerations, the Organisation must conduct their security intelligence activities in accordance with Ministerial Guidelines. This includes, among other things, that the Organisation’s actions should be proportionate to the gravity of the threat posed and the probability of its occurrence, and that inquiries and investigations should be done with as little intrusion into privacy as possible.

**Summary**

51. When an IPO is sought by *enforcement agencies, control order IPO agencies*, and the Organisation, the decision maker or nominated AAT Security Division member must evaluate the individual circumstances of each application. They must balance the effectiveness of the agency applying for an IPO, as well as wider public interests, such as the impact on privacy. To assist the decision maker or nominated AAT Security Division member reach a decision in connection with an application, they have the discretion to seek from the relevant agency additional information to further inform their assessment of the application before them.

52. Therefore, the amendments allowing *enforcement agencies, control order IPO agencies*, and the Organisation to apply for IPOs related to stored communications and *telecommunications data* do not constitute arbitrary or unlawful interference with a person’s privacy. To the extent that there is a limitation on the protection against arbitrary or unlawful interference with a privacy, statutory safeguards ensure any interference is reasonable, necessary and proportionate.

**Incoming orders and requests**

53. Part 13 of the Schedule forms part of the framework to support situations whereby governments of foreign countries that have a designated international agreement with Australia may seek communications data from Australian communications providers. Part 13 excludes the prohibitions in the TIA Act and the *Telecommunications Act 1997* and authorises disclosures for the purposes of the *Privacy Act 1988* to the extent the disclosure is in accordance with an incoming order or request (referred to as ‘blocking provisions’).

54. This Part removes these blocking provisions for a purpose that is authorised by the Bill and for no other purpose. Therefore, the protections of the blocking provisions continue to have effect generally in law and are not set aside.
55. The removal of blocking provisions is reasonable and necessary in the circumstances, as it ensures Australian communications service providers are not be prevented from responding to requests for communications data by foreign governments with which Australia has a designated international agreement, and which are expected to operate under the principle of reciprocity. These measures are permissive in nature, and place no obligations under Australian law on Australian communications service providers to provide data in response to an incoming request.

56. If Part 13 did not form part of the Bill, Australian communications providers may not be able to disclose information with foreign partners with whom Australia has an agreement and where an underlying order to do so is in place. This Part does not diminish the responsibility of Australian communications providers to comply with privacy obligations in providing information to foreign parties. For the reasons identified above, the protection against arbitrary or unlawful interference with privacy under Article 17 of the ICCPR are appropriately and permissibly limited.

Disclosure of protected information

57. Part 11 of the Bill prohibits the disclosure of information obtained under an IPO issued under Parts 2, 3 or 4 except in certain circumstances.

58. The circumstances in which information may be disclosed are outlined throughout Part 11 of Schedule 1 of the TIA Act and include, but are not limited to, the investigation or prosecution of relevant serious offences, the making of reports and keeping of records under Part 10 of Schedule 1 of the TIA Act, inspections by the Commonwealth Ombudsman, and for the purposes of a designated international agreement.

59. Noting the specific limited circumstances outlined throughout Part 11 and the relevance to the operation of the framework established in the Bill, the use of information obtained under an IPO promotes the privacy of individuals as it does not permit the use of information for a purpose not relevant to achieving a legitimate purpose of the Bill.

Destruction of records

60. Section 140 of Schedule 1 of the TIA Act requires the destruction of information obtained under IPOs issued in Parts 2, 3 and 4 for interception activities and stored communications.

61. The information must be destroyed by the chief officer of the relevant agency which is in possession of the information if the chief officer is satisfied the information is not likely to be required for a permitted purpose identified in Part 11.

62. The destruction of information obtained under an IPO seeking telecommunications data is not required by this section in line with current arrangements in the TIA Act. This view is supported by the Attorney-General’s Department in their response to recommendation 28 of the Parliamentary Joint Committee on Intelligence and Security’s Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. Among other things, the Attorney-General’s Department’s response found:
• Keeping telecommunications data for extended periods of time can be beneficial to law enforcement agencies in particular circumstances.

• A destruction requirement may have little privacy benefit and could create a further burden on the telecommunications industry.

• It will be administratively challenging to destroy copies of telecommunications data given its need to be stored on numerous information management systems.²

63. Requiring the destruction of records ensures the private communications of individuals subject to an IPO are not kept in perpetuity where there is no legitimate reason to do so. This measure serves to limit the scope of the interference with an individual's privacy by ensuring the power to retain information is appropriately focused on achieving a legitimate purpose under the Bill. On this basis, the provision serves to enhance the protection against arbitrary or unlawful interference with privacy in circumstances where they are subject to an IPO.

**Right to freedom of expression - Article 19 of the ICCPR**

64. Article 19(2) of the ICCPR provides everyone shall have the right to freedom of expression, including the right ‘to seek, receive and impart information and ideas of all kinds and regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice’.

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

66. The framework may engage the right to freedom of expression by indirectly making some people more reluctant to use communications services. It is plausible that a person may minimise their use of communication services if they know government agencies can seek designated communications providers to provide communications carried through these services.

67. However, the amendments will not enable agencies to access communications absent an order. IPOs are subject to strict thresholds, for example, they can only be issued in relation to stored communications and telecommunications data to detect, prevent, investigate or prosecute serious offences attracting a maximum penalty of at least 3 years imprisonment, or life imprisonment. This approach is consistent with the current domestic warrant regime under the TIA Act, and the mutual legal assistance regime.

68. The framework advances a legitimate objective of protecting Australia’s national security and public order by allowing law enforcement and national security agencies to respond to the modern communications environment and effectively access information that will assist investigations and prosecutions.

² Attorney-General’s Department, June 2017, ‘Review of the adequacy of destruction requirements for telecommunications data’.
69. To the extent that a person refrains from or minimises their use of electronic communications in response to this framework, the circumstances under which IPOs may be issued ensure any limitation on the freedom of expression is necessary and proportionate. Additionally, to the extent that the framework does limit the right to freedom of expression, such a limitation is contemplated by the ICCPR as Article 19(3) allows for restrictions for the protection of national security or of public order.

**Right to life - Article 6 of the ICCPR**

70. Article 6(1) of the ICCPR protects the inherent right to life and the right to not be arbitrarily deprived of life.

71. The Bill enables Australia to designate agreements with governments of foreign countries for the purpose of obtaining communications data to be able to investigate and prosecute serious criminal offences. These agreements are expected to operate under the principle of reciprocity. As governments of foreign countries are responsible for their own criminal offences, it may be contemplated that Australia designates an agreement with a foreign country where death is the penalty for certain serious criminal offences and therefore, in accordance with the framework of the Bill, enables communications providers in Australia to provide communications data to that foreign government for the purpose of prosecuting a person for an offence for which the death penalty relates.

72. The Bill prohibits the Minister from specifying a designated agreement for the purpose of the Bill except in circumstances where the Minister has received, from the government of a foreign country, a written assurance relating to the use or non-use of information obtained under the framework of the Bill in any proceeding by way of prosecution for an offence for which death is the penalty.

73. Australia’s long standing bipartisan opposition to the death penalty is well-known and Australia opposes the death penalty in all circumstances for all people. Requiring governments of foreign countries to provide a written assurance acknowledges the right to life is engaged by the Bill as it does not permit an agreement to be specified where no assurance is given. The decision to specify an agreement is not left to the discretion of the Minister as the relevant provisions in the Bill place an obligation on the Minister to not specify an agreement where no assurance is given.

74. Owing to the restriction on the Minister’s ability to designate agreements with governments of foreign countries in relation to the provision of a written assurance, the right to life under Article 6 of the ICCPR is recognised.

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

75. Article 2(3) of the ICCPR protects the right to an effective remedy for any violation of rights and freedoms recognised by the ICCPR, including the right to have such a remedy determined by competent judicial, administrative or legislative authorities or by any other competent authority provided for by the legal system of the State. To the extent that a legal entity subject to an IPO argues that complying with the order would infringe the rights of natural persons affected by compliance with the order, the remedies discussed here are applicable.
76. Judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) is not available for decisions made under the TIA Act. This is consistent with similar decisions made for national security and law enforcement purposes – for example those made under the *Intelligence Services Act 2001*, the *Australian Security and Intelligence Act 1979*, and certain decisions made under the *Telecommunications Act 1997*. Decisions of a law enforcement nature were identified by the Administrative Review Council in its publication ‘What decisions should be subject to merits review?’ as being generally unsuitable for merits review.

77. Australian courts will retain jurisdiction for judicial review of a decision of a decision maker or nominated AAT Security Division member to issue an IPO, through the original jurisdiction of the High Court of Australia and in the Federal Court of Australia by operation of subsection 39B(1) of the *Judiciary Act 1903*. This will ensure that an affected person or a provider has an avenue to challenge unlawful decision making.

78. As IPOs are intended to be used without the knowledge of the person of interest, so as not to jeopardise an investigation or prosecution, challenges to an application will generally not be able to take place at the same time an application for an IPO is made. However, the decision to issue an IPO may be challenged by a defendant during court proceedings on the basis that the evidence was improperly or illegally obtained. The court has the discretion not to admit such evidence should a challenge on this basis be successful.

79. Oversight by the Commonwealth Ombudsman will also provide for an effective mechanism to ensure agency use of the powers in the Bill is compliant with the terms of the legislation, thereby bolstering the proper use of framework. The power to inspect agency records, and the obligation to provide reports to the Minister on the results of those inspections is contained in Part 10 of the Bill. The Minister is obliged to table the report in Parliament. The Inspector-General of Intelligence and Security will automatically have oversight over the Organisation’s compliance with the scheme under its existing legislation.

80. To the extent a person’s right to an effective remedy for the violation of their human rights under the ICCPR is restricted by the limitations in the ADJR Act, those limitations are reasonable, necessary and proportionate.

Conclusion

81. This Bill is compatible with human rights as set out above and promotes the protection of several rights. To the extent that the Bill limits a human right, those limitations are reasonable, necessary and proportionate.
NOTES ON CLAUSES

Preliminary

Section 1 - Short title

1. This clause provides for the short title of the Act to be the *Telecommunications Legislation Amendment (International Production Orders) Act 2020* (the Act).

Section 2 - Commencement

2. Subsection 2(1) provides for the commencement of each provision in the Act, as set out in the table contained in this subclause.

3. Item 1 of the table provides that sections 1 to 3, and anything in the Act not elsewhere covered by the table, commence on the day this Act receives Royal Assent.

4. Item 2 of the table provides Parts 1 and 2 of Schedule 1 commence on the day after this Act received Royal Assent.

5. Item 3 of the table provides Part 3 of Schedule 1 commences on the later of
   - immediately after the commencement of the provisions covered by table item 2; and
   - the commencement of the *Federal Circuit and Family Court of Australia Act 2020*.

6. However, Part 3 of Schedule 1 does not commence at all if the event mentioned at paragraph (b) does not occur.

7. Item 4 provides Part 4 of Schedule 1 commences on the day after this Act receives Royal Assent.

8. A note on the table establishes that this table relates only to the provisions of this Act as originally enacted. This table will not be amended to deal with any later amendments of this Act.

9. Subclause 2(2) clarifies that any information in column 3 of the table is not part of this Act. This subclause sets out that information may be inserted in this column, or information in it may be edited, in any published version of this Act.

Section 3 - Schedules

10. This clause provides each Act that is specified in a Schedule is amended or repealed as set out in that Schedule and that any other item in the Schedule has effect according to its terms.
Schedule 1 - Amendments

Part 1 – General Amendments

Australian Crime Commission Act 2002

Item 1  Paragraph 19A(5)(d)

11. This item adds the prohibition on use, recording, communication, or publication of protected information obtained in the provisions of item 43 of this Bill to the powers of an Examiner under the *Australian Crime Commission Act 2002* to request information from agencies.

Item 2  Schedule 1

12. This item adds the prohibition on use, recording, communication, or publication of protected information obtained in the provisions of item 43 of this Bill to the meaning of prescribed provision in the *Australian Crime Commission Act 2002*.

Australian Security Intelligence Organisation Act 1979

Item 3  At the end of section 18

13. This item adds provisions to permit the communication of intelligence for the purpose of provisions in item 43 of the Bill.

Item 4  After subsection 94(2BB)

14. This item inserts reporting requirements into the existing annual reporting provision in the *Australian Security Intelligence Organisation Act 1979*. These reporting requirements relate to the Organisation’s use of relevant provisions in item 43 of this Bill.

15. This item clarifies for the purpose of the reporting requirements, the meaning of terms used have the same meaning as they do in item 43 of this Bill.

Freedom of Information Act 1982

Item 5  Schedule 3

16. This item adds the prohibition on use, recording, communication, or publication of protected information obtained in provisions of item 43 of this Bill to Schedule 3 of the *Freedom of Information Act 1982*. This has the effect that if item 43 of this Bill prohibits the disclosure of information contained in a document, that document is an exempt document under section 38 of the *Freedom of Information Act 1982*.

International Criminal Court Act 2002

Item 6  After subsection 69A(1)

17. This item inserts provisions to permit the Attorney-General to authorise the provision of material to the International Criminal Court that includes protected information obtained in accordance with an IPO issued under Part 2 or Part 3 of this Schedule. If the protected
information was obtained in accordance an IPO relating to interception issued under clause 30 or 60, then it can only be provided if the Prosecutor’s investigation or International Criminal Court proceeding relates to an offence punishable by a maximum term of imprisonment of 7 years or more, or life.

**Item 7**  
**Subsection 69A(2)**

18. This item clarifies the conditions extend to amendments made in item 6 of the Bill.

*Law Enforcement Integrity Commissioner Act 2006*

**Item 8**  
**Subsection 5(1) (paragraph (c) of the definition of law enforcement secrecy provision)**

19. This item adds the prohibition on use, recording, communication, or publication of protected information obtained in provisions of item 43 of this Bill to the definition of law enforcement secrecy provision.

*Mutual Assistance in Criminal Matters Act 1987*

**Item 9**  
**Subsection 3(1)**

20. This item inserts the definition of International Production Order in the Mutual Assistance in Criminal Matters Act 1987.

**Item 10**  
**Subsection 3(1)**

21. This item repeals the definition of protected information.

**Item 11**  
**Subsection 3(1)**

22. This item inserts definitions for protected information that distinguishes between the existing definition of protected information in particular parts of the Surveillance Devices Act 2004, and protected information within the meaning of provisions in item 43 of the Bill. The definitions are broken down by protected IPO intercept information, protected IPO stored communications information, protected IPO telecommunications data information, protected SD information, and telecommunications data.

**Item 12**  
**Subsection 13A(2) (table item 1, column 1)**

23. This item omits reference to protected information in Column 1 of the table and substitutes protected SD information.

**Item 13**  
**Subsection 13A(2) (at the end of the table)**

24. This item amends the table to include items 4 and 5. Item 4 permits the Attorney-General to authorise the provision of protected IPO intercept information relevant to a serious offence punishable by a maximum penalty of imprisonment for 7 years or life or the death penalty. Item 5 permits the Attorney-General to authorise the provision of protected IPO stored communications information or protected IPO telecommunications data information relevant to a serious offence punishable by a maximum penalty of imprisonment for 3 years or life or the death penalty.
25. This amendment broadens the material which the Attorney-General may authorise to be provided to a requesting foreign country under the *Mutual Assistance in Criminal Matters Act 1987* framework to include material obtained under provisions in item 43 of the Bill.

*Telecommunications (Interception and Access) Act 1979*

**Item 14** Title

26. This item amends the long title of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) by replacing the phrase “and for related purposes” with “and for other purposes”.

27. This amendment is consequential to the main amendments introduced by the Bill, which introduce a Schedule 1 to the TIA Act relating to IPOs. These amendments will form part of the TIA legislative framework, but are not specifically related to the original purpose of the TIA Act, as set out in the long title of the TIA Act.

**Item 15** Subsection 5(1) (at the end of the definition of access)

28. The Bill inserts a number of definitions of terms in Schedule 1 (see item 43) which are also defined in the TIA Act as it currently stands. The purpose of this and other similar items is to highlight that certain terms in the TIA Act will have different definitions, depending on their location in either the main part of the TIA Act or in Schedule 1 (as added by the Bill).

29. This item provides the definition of access to be added by the Bill applies only in relation to Schedule 1 and not to the main part of the TIA Act, which has its own definition of that term (see subsection 5(1) of the TIA Act).

**Item 16** Subsection 5(1) (definition of carriage service provider)

30. This item provides the definition of carriage service provider to be added by the Bill (see item 43) applies only in relation to the Schedule 1 and not to the main part of the TIA Act, which has its own definition of that term (see subsection 5(1) of the TIA Act).

**Item 17** Subsection 5(1) (paragraph (a) of the definition of carrier)

31. This item provides the definition of carrier to be added by the Bill applies only in relation to the Schedule 1 and not to the main part of the TIA Act, which has its own definition of that term (see subsection 5(1) of the TIA Act).

**Item 18** Subsection 5(1) (at the end of the definition of carrier)

32. This item adds paragraph (c) to the existing definition of carrier in the TIA Act, to provide that, for the purposes of Schedule 1, carrier has the meaning given by clause 2 of Schedule 1.

**Item 19** Subsection 5(1) (definition of equipment)

33. This item provides the existing definition of equipment in the TIA Act does not apply in relation to Schedule 1, as added by the Bill. This is to ensure that the definition of equipment in this Schedule reflects the context in which IPOs are issued. Specifically, this
definition intends to link itself more closely with the functions of an individual carriage service, rather than a telecommunications network.

**Item 20**  
**Subsection 5(1) (definition of intended recipient)**

34. This item provides the definition of *intended recipient* to be added by the Bill applies only in relation to the Schedule 1, and not to the existing TIA Act, which has its own definition of that term (see subsection 5(1) of the TIA Act). The definition of *intended recipient* in Schedule 1 is intended to apply in relation to individual carriage services, rather than a telecommunications service. The Schedule intends to capture intended recipients that are using a carriage service, rather than limit the application of the definition to circumstances where the intended recipient is only using a telecommunications service. Circumstances that only involve the use of a telecommunications service are limited to the collection of interception material, whereas this Schedule of the Bill intends to apply the definition of *intended recipient* to interception material, stored communications and telecommunications data that is requested under an IPO.

**Item 21**  
**Subsection 5(1) (definition of issuing authority)**

35. This Item provides the definition of *issuing authority* to be added by Schedule 1 in item 43 of the Bill applies only in relation to the Schedule and not to any other part of the TIA Act.

**Item 22**  
**Subsection 5(1) (at the end of the definition of lawfully accessed information)**

36. This item amends the definition of *lawfully accessed information* in subsection 5(1) of the TIA Act, to provide that it does not include information obtained in accordance with an IPO (within the meaning of Schedule 1). This is to ensure that none of the functions created under the Bill are unnecessarily affected by portions of the TIA Act that relate to stored communications information, which separates the current domestic regime from the IPO regime.

**Item 23**  
**Subsection 5(1) (definition of nominated AAT member)**

37. This item inserts the definition of *nominated AAT Security Division member* to mean a member of the AAT in respect of whom a nomination is in force under section 6DAA to issue IPOs under Part 4 of Schedule 1, as added by the Bill.

**Item 24**  
**Subsection 5(1) (definition of record)**

38. This item seeks to quarantine the existing definition of *record* so that it does not apply to provisions in item 43 of the Bill. The meaning of *record* in the TIA Act relates to interception within the context of the Australian telecommunications systems. Interception in item 43 of the Bill will be dealt with in isolation of the TIA Act to preserve this notion.

**Item 25**  
**Subsection 5(1) (definition of relevant statistics)**

39. This item provides the existing definition of *relevant statistics* in the TIA Act does not apply in relation to Schedule 1, as added by the Bill. This is to enable annual reporting on the use and effectiveness of IPOs issued under Parts 2, 3, and 4 of Schedule 1, to be appropriately suited to the framework established in Schedule 1 of the Bill.
Item 26  Subsection 5(1) (definition of stored communication)

40. This item provides the existing definition of \textit{stored communication} in the TIA Act does not apply in relation to Schedule 1, as added by the Bill. This serves to de-conflict the operation of the Schedule contained in the Bill from the existing functions of the TIA Act, as they relate to accessing stored communications information.

Item 27  Subsection 5(1) (definition of telecommunications network)

41. This item provides the existing definition of \textit{telecommunications network} in the TIA Act does not apply in relation to Schedule 1, as added by the Bill. The definition of \textit{telecommunications network} contained within the Bill is intended to be technology neutral and can apply to future iterations of technology that become capable of carrying communications by means of guided and/or unguided electromagnetic energy.

Item 28  Subsection 5(1) (definition of telephone application)

42. This item provides the existing definition of \textit{telephone application} in the TIA Act does not apply in relation to Schedule 1, as added by the Bill. The definition of \textit{telephone application} contained within the Bill is intended to apply in relation to IPOs, which is not covered by the TIA Act definition of \textit{telephone application}.

Item 29  Section 5A

43. This item provides existing section 5A of the TIA Act, which relates to communicating etc. information obtained by interception does not apply in relation to Schedule 1 of item 43 of the Bill. Section 5A of the TIA Act relates to interception within the context of the Australian telecommunications systems. Interception in item 43 of the Bill will be dealt with in isolation of the TIA Act to preserve this notion.

Item 30  Section 5F

44. This item provides existing section 5F of the TIA Act, which relates to when a communication is passing over a telecommunications system, does not apply in relation to Schedule 1, as added by the Bill. The application of section 5F of the TIA Act relies on the definition of telecommunications system linking back to a telecommunications network, both concepts that this Bill does not rely on. As such, the key features of the types of information that can be requested are contained within each section respectively.

Item 31  Section 5G

45. This item provides existing section 5G of the TIA Act, which relates to the intended recipient of a communication, does not apply in relation to Schedule 1, as added by the Bill. The application of section 5F of the TIA Act relies on the definition of telecommunications system linking back to a telecommunications network, both concepts that this Bill does not rely on. As such, the key features of the types of information that can be requested are contained within each section respectively. The definition of \textit{intended recipient} in Schedule 1 is intended to apply in relation to individual carriage services, rather than a telecommunications service. The Schedule intends to capture intended recipients that are using a carriage service, rather than limit the application of the definition to circumstances where the intended recipient is only using a telecommunications service. Circumstances that only involve the use of a telecommunications service are limited to the collection of
interception material, whereas this Schedule of the Bill intends to apply the definition of *intended recipient* to interception material, stored communications and telecommunications data that is requested under an IPO.

**Item 32  Subsection 6(1)**

46. This item provides existing subsection 6(1) of the TIA Act, which relates to interception of a communication, does not apply in relation to Schedule 1, as added by the Bill. The Schedule intends to capture interception of a communication in the related section that details the requirements for an IPO for stored communications, rather than rely on a broad overarching definition that leans on the depiction of telecommunications system.

**Item 33  Subsection 6D(1) (definition of eligible judge)**

47. This item repeals the existing definition of eligible judge and substitutes a new definition to mean: (a) except when used in Schedule 1 (as added by the Bill)—a Judge in relation to whom a consent under subsection 6D(2) and a declaration under subsection 6D(3) are in force; and (b) when used in Schedule 1 (as added by the Bill)—to mean a Judge in relation to whom a consent under subclause 14(2) of Schedule 1 (as added by the Bill) and a declaration under subclause 14(3) (as added by the Bill) are in force.

**Item 34  Subsection 6D(3) and (4)**

48. This item provides existing subsection 6D(3) of the TIA Act, which relates to the Attorney-General declaring certain Judges to eligible Judges for the purposes of the TIA Act, does not apply in relation to Schedule 1, as added by the Bill. Clause 29 of Schedule 1 (as added by the Bill) provides for the Attorney-General to declare certain Judges to eligible Judges for the purposes of the Schedule 1.

**Item 35  After subsection 6DB(3)**

49. This item inserts subsection 6DB(3A). Subsection 6DB(1) contains provisions with respect to the Attorney-General appointing, by writing, an issuing authority. Subsection 6DB(3A) provides an appointment made under subsection 6DB(1) has no effect for the purposes of Schedule 1, as added by the Bill. Instead, clause 16 of Schedule 1, as added by the Bill, provides for the Attorney-General to appoint an issuing authority for the purposes of Schedule 1.

**Item 36  Subsection 6DB(4)**

50. This item provides the existing subsection 6DB(4) of the TIA Act does not apply in relation to Schedule 1, as added by the Bill. Instead, clause 16(5) of Schedule 1, as added by the Bill, similarly provides an issuing authority has, in relation to the performance or exercise of a function or power conferred on an issuing authority by Schedule 1, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

**Item 37  Subsection 6E(1)**

51. This item is consequential to the amendment made in item 38.
Item 38  
At the end of section 6E

52. This item adds subsection 6E(3). Section 6E deals with lawfully intercepted information. Subsection 6E(3) provides a reference in the Act to lawfully intercepted information does not include a reference to information obtained in accordance with an IPO (within the meaning of Schedule 1, as added by the Bill). This is to preserve the meaning of lawfully intercepted information in the TIA Act as it relates to interception within the context of the Australian telecommunications systems.

Item 39  
Section 6P

53. This item amends section 6P, which deals with the identification of a service, to provide that the provisions in this section do not apply to Schedule 1, as added by the Bill.

Item 40  
After paragraph 7(2)(bb)

54. This item inserts paragraph 7(2)(bc). Subsection 7(2) relates to exemptions from the general prohibition in subsection 7(1) to the interception of telecommunications. Paragraph 7(2)(bc) introduces a new exemption, being an act or thing done in compliance with an IPO (within the meaning of Schedule 1, as added by the Bill).

Item 41  
After paragraph 108(2)(cb)

55. This item inserts paragraph 108(2)(cc). Subsection 108(2) relates to exemptions from the general prohibition in subsection 108(1) on access to stored communications. Paragraph 108(2)(cc) introduces a new exemption, being an act or thing done in compliance with an IPO (within the meaning of Schedule 1, as added by the Bill).

Item 42  
After section 299

56. This item inserts section 299A, which relates to Schedule 1, as added by the Bill. This is a technical item, which provides Schedule 1 has effect.

Item 43  
At the end of the Act

57. This item adds Schedule 1 – IPOs to the TIA Act. A note inserted by this item refers to section 299A inserted by item 42 of the Bill.
Schedule 1 - International Production Orders

Part 1 - Introduction

58. Clause 1 provides a simplified outline of Schedule 1 of the TIA Act, as inserted by the Bill. It briefly describes the framework for issuing IPOs directed to designated communications providers, and for enabling the exemption from Commonwealth laws restricting interception or disclosure, acts or things done in compliance with corresponding orders issued by a competent authority, in accordance with a designated international agreement.

59. Clause 2 provides the definitions for many of the terms which have a particular meaning under Schedule 1 of the TIA Act.

a. **access** is defined as including access subject to a pre-condition (such as the use of a password), access by way of push technology and access by way of standing request. Push technology involves access that is not initiated by an end-user (pull technology). For example, a user could be presented with a message notification that they have not intentionally accessed and is displayed automatically and this would be considered **access**. This is consistent with the definition used in the *Enhancing Online Safety Act 2015* and Part 15 of the *Telecommunications Act 1997*.

b. **account** is broadly defined as including a free account, a pre-paid account and anything that may reasonably be regarded as the equivalent of an account. This is intended to ensure the definition applies to possible future circumstances where the ordinary understanding of what constitutes an account shifts and changes along with relevant technological changes. This is consistent with the definition used in the *Enhancing Online Safety Act 2015*.

c. **ASIO official** is defined to mean the Director General of Security; or an ASIO employee; or an ASIO affiliate. This definition is intended to ensure the Bill’s record keeping requirements regarding ASIO apply to each of these kinds of individuals.

d. **Attorney General’s Department** is defined to mean the Department administered by the Attorney General.

e. **Australian Designated Authority** is defined to mean the Secretary of the Attorney General’s Department.

f. **carriage service** is defined to be consistent with the definition used in the *Telecommunications Act 1997*. This definition is intended to broadly capture any current or future services that facilitate the transmission of communications through a wide variety of technological means.

g. **carriage service provider** is defined broadly to mean a person who supplies a carriage service to the public or a section of the public. This definition is intentionally broader than the definition of **carriage service provider** in section 87 of the *Telecommunications Act 1997* and does not require a nexus to Australia. However, the definition is intended to ensure an IPO could not be issued to communications providers who only provide a service internally within their organisation, such as an intranet system, whilst also capturing providers that do provide a service to an external section of the public.
h. **carrier** is defined broadly to mean a person who owns or operates a telecommunications network that is used to supply a carriage service to the public or a section of the public. The definition of *telecommunications network* when used in Schedule 1 of the TIA Act is not limited to a telecommunications network that is within Australia, or partly within Australia. An example of a carrier may be a foreign company who owns network units that deliver carriage services. Such facilities could include transmission infrastructure, cabling, and wireless networks.

i. **certified copy** is defined to have the meaning giving by clauses 174 to 178 of this Schedule. In line with clauses 174 to 178 certified copies are to be received in evidence as a true copy of the IPO.

j. **control order IPO agency** is defined to include those agencies within the definition of *control order agency* already contained within the TIA Act.

k. **designated communications provider** is defined to mean a carrier, or a carriage service provider, or a message/call application service provider, or a storage/back-up service provider, or a general electronic content service provider. This definition covers additional kinds of entities to those set out at section 317C of the *Telecommunications Act 1997*. A designated communications provider does not require a connection to Australia, recognising the operation of the designated international agreements. Individuals, as well as body corporates, may be designated communications providers.

l. **designated international agreement** is defined in clause 3. Clause 3 sets out the requirements in terms of designating an international agreement for the purposes of this Schedule.

m. **eligible judge** is defined to be given meaning by clause 3 of the Bill.

n. **general electronic content service** is defined to have the meaning given by clause 4A of the Bill.

o. **general electronic content service provider** is defined to mean a person who provides a general electronic content service to the public or a section of the public. This captures any provider who provides a service that allows end-users to access material using a carriage service, or delivers material to persons having equipment appropriate for receiving that material. An example of this includes a service that permits the public to post *content* either available to the broader public or a section of the public. This would capture circumstances where a person provides a website that contains private or public forums that may facilitate the sharing of information or content.

p. **individual carriage service** is defined as a carriage service that is supplied using a particular telecommunications identifier. This definition is used to ensure that for an IPO in respect of carriage services, the carriage service must be identifiable. For example, a particular internet service identifiable by a unique telecommunications identifier (e.g. account name or IP address) offered by an internet service provider would be an individual carriage service.

q. **individual message/call application service** is defined as a message/call application service to the extent to which the service is provided using a particular
telecommunications identifier. This definition is used to ensure that for an IPO in respect of individual message/call application services, the individual message/call application service must be identifiable. For example, an over-the-top messaging application that allows for a person to communicate with other persons identifiable by a unique telecommunications identifier (unique account identifier, or mobile device identifier attached to that message application installed on the mobile device).

r. **intended recipient** is defined to have the meaning given by clause 5A.

s. **intercept** is defined to mean record or live stream to a single destination. The inclusion of live streaming recognises that unlike traditional telecommunication interception warrants, the person required to comply with an IPO may operate differently, and may not involve agency officers listening to the communication as it passes their telecommunications network. However, the person required to comply with an IPO may be required to live stream the communication to a single destination to facilitate the agency officer to listen to that communication.

t. **International Production Order** is defined to mean an IPO issued under this Schedule.

u. **issuing authority** is defined to mean a person in respect of whom an appointment is in force under clause 5F.

v. **manager** is defined to mean the chief executive officer (however described) of the provider; or any other individual who is involved in the management of the provider. This is intended to be flexible depending on the designated communications provider to ensure that the authorisation of evidentiary certificates is not an onerous process but has sufficient seniority to authorise evidentiary certificates for that particular designated communications providers.

w. **material** is defined broadly to capture current and future forms of electronic information.

x. **member of staff of the Attorney General’s Department** is defined to mean either the Secretary of the Attorney General’s Department; or an Australian Public Service employee in that Department.

y. **message** is defined broadly to capture current and future forms of a message.

z. **message application service** is defined to have the meaning given by clause 3A of the Bill.

aa. **message/call application service** is defined broadly to include message, voice call and video call application services.

bb. **message/call application service provider** is defined as a person who provides a message/call application service to the public or a section of the public. This term encompasses application services that enable end-users to send or receive communications to or from one another using a carriage service.
cc. **nominated AAT member** is defined to mean a member of the AAT in respect of whom a nomination is in force under clause 5E to issue IPOs under Division 2 of Part 2, and Division 2 of Part 3, of this Schedule.

dd. **nominated AAT Security Division member** is defined to mean a member of the AAT in respect of whom a nomination is in force under clause 5G to issue IPOs under Part 3 of this Schedule.

ee. **posted** on a general electronic content service is defined to have the meaning given by clause 4B of the Bill.

ff. **protected information** is defined to include all information obtained by reason of compliance with Schedule 1 of the TIA Act that requires protection from unauthorised use and disclosure.

gg. **relevant agency** is defined to mean an interception agency; or a criminal law enforcement agency; or an enforcement agency; or a control order IPO agency.

hh. **relevant statistics** is exhaustively defined, in relation to applications of a particular kind, to include how many applications were made, withdrawn, refused, and how many IPOs were issued in response to applications of that kind. This definition is intended to reflect the relevant statistic definition contained under section 5 of the TIA Act.

ii. **serious category 1 offence** is defined to mean an offence that is punishable by a maximum term of imprisonment of 3 years or more or for life. This reflects the minimum threshold for offences that can be the subject of a stored communications warrant.

jj. **serious category 2 offence** is defined to mean a serious offence or an offence that is punishable by a maximum term of imprisonment of 7 years or more or for life, or a serious offence at section 5D of the TIA Act. This reflects the minimum threshold for offences that can be the subject of a telecommunications interception warrant.

kk. **service** is defined to include a website and does not apply to the definition of **carriage service**.

ll. **storage/back-up service** is defined to have the meaning given by clause 7.

mm. **storage/back-up service provider** is defined to mean a person who provides a storage/back-up service to the public or a section of the public. An example of this would be a cloud-storage solutions provider who provides the ability for the public to remotely store material for storage or back up purposes.

nn. **stored communications** has a meaning similar to stored communications as defined in subsection 5(1) of the TIA Act, but is broadened to include material that is uploaded for storage/back-up or posted. The definitions in subparagraph (ii) of paragraphs (a) and (b) has been included to clearly distinguish stored communications from interception.

oo. **telecommunications data** includes information or documents that are not the content of a communication or material. For example, telecommunications data generally falls
into two categories: information that allows a communication to occur (such as the time and date of a communication, or the duration of the communication), and information about the parties to the communication (such as the name of the customer, billing information, contact details, and account information). It may also go to identifying a service. This reflects the types of information that can be authorised to be disclosed under Chapter 4 of the TIA Act.

pp. **telecommunication identifier** refers to information that can be used to identify a relevant service.

qq. **telecommunications network** is defined to mean a system, or series of systems, that carries, or is capable of carrying, communications by means of guided and/or unguided electromagnetic energy. This is similar to the definition of **telecommunication network** in subsection 5(1) of the TIA Act but does not exclude systems for carrying communications solely by means of radiocommunication.

rr. **telephone application** is defined to mean an application made by telephone for an IPO.

ss. **telephone number** is defined to include a mobile telephone number.

tt. **uploaded** is defined to have a meaning affected by clause 5.

uu. **use** is defined to have a meaning affected by clause 5.

vv. **video call** is defined to have a meaning that includes a video call that has an audio component.

ww. **video call application service** is defined to have a meaning given by clause 3C.

xx. **voice call** is defined to include a call that involves a recorded or synthetic voice.

yy. **voice call applications service** is defined to have a meaning given by clause 3B.

**Designated international agreement**

60. Clause 3 provides the definition for a *designated international agreement*.

61. Subclause 3(1) provides, for a bilateral agreement to be a *designated international agreement*, it must be an agreement that is between Australia and a foreign country, that is specified in the regulations and has come into force. Any regulations made under subclause 3(1) will be legislative instruments and subject to disallowance.

62. Subclause 3(2) places limits on when a bilateral agreement may be specified in the regulations. If one or more offences against the law of the foreign country party to the agreement are punishable by death, and the agreement deals with orders, warrants, authorisations or other process from an authority of the foreign country then, before the agreement can be specified in the regulations, the Minister must have received a written assurance from the government of the foreign country about the use or non-use of Australian-sourced information in any proceeding by way of prosecution for an offence that is punishable by death in the foreign country.
63. This written assurance may be contained in a single written document, or across a number of documents, such as the text of the agreement, a letter or exchange of letters, or a record of understanding or memorandum of understanding. The written assurance may deal with how Australian-sourced information may be used by the foreign country in proceedings in connection with prosecutions for death penalty offences, including for exculpatory purposes, and subject to any restrictions or conditions, or it may deal with how Australian-sourced information is not to be used in prosecutions for death penalty offences, or a combination of both.

64. This provision is designed to be flexible as to the form, content and nature of the written assurance to be received as this will depend on the particular foreign country and the particular agreement. The policy intention of this provision is to give effect to Australia’s long-standing bipartisan opposition to the death penalty in the context of reciprocal cross-border access to communications data, and complements existing death penalty safeguards across the full spectrum of Australia’s international crime cooperation frameworks. The Bill prohibits the Minister from specifying a designated agreement for the purpose of the Bill except in circumstances where the Minister has received, from the government of a foreign country that has laws including an offence attracting the death penalty, a written assurance relating to the use or non-use of information obtained under the framework of the Bill in any proceedings by way of prosecution for such an offence.

65. Subclause 3(3) provides, for a multilateral agreement to be a designated international agreement, it must be an agreement that is between Australia and two or more foreign countries that is specified in the regulations and has come into force.

66. Subclause 3(4) provides, for a multilateral agreement, the regulations may declare that one or more of the party foreign countries are recognised parties to the agreement for the purposes of this Schedule.

67. Subclause 3(5) places limits on when a foreign country may be declared as a recognised party to the agreement for the purposes of the agreement under subclause 3(4). If one or more offences against the law of one or more foreign country parties to the agreement are punishable by death, and the agreement deals with orders, warrants, authorisations or other process (however described) from an authority of the foreign country then, before the country can be specified in the regulations as a recognised party, the Minister must have received a written assurance from the government of the foreign country about the use or non-use of Australian-sourced information in any proceeding by way of prosecution for an offence that is punishable by death in the foreign country.

68. Subclause 3(6) provides the Schedule will not have effect in relation to foreign countries that are not declared as recognised parties to the relevant multilateral designated international agreement. This is intended to permit the Schedule to apply to parties to multilateral agreements that do not have offences punishable by death, or that provide the Minister with a written assurance in line with subclause 3(5). In regulations, the Minister may declare or remove foreign countries as recognised parties to the agreement, including in the event that a country party introduces or abolishes the death penalty, provides an assurance at a later time, or a new country with the death penalty becomes a party to the agreement.

69. Subclause 3(7) provides the Minister must announce, by notifiable instrument, the day an agreement under this clause enters into force for Australia.
70. Subclause 3(8) identifies when information obtained in accordance with an order is Australian-sourced information. This definition is intended to capture a range of circumstances in which the information might reasonably be considered to have been sourced from Australia pursuant to an order, warrant, authorisation or other request. These circumstances are where the order requires something to be done in Australia, or if the order is directed to an individual in Australia, or a body corporate that is incorporated in Australia, or a body established by or under a Commonwealth, state or territory law.

71. The text of each designated international agreement will be able to be viewed in the Australian Treaties Library on the Austlii website: www.austlii.edu.au

Message application service

72. Clause 4 provides the definition for a message application service. Subclause 4(1) provides a message application service means any service that enables end users to send or receive messages to or from other end-users using a carriage service. Current examples of a message application service including the services offered by Kik Messenger and WhatsApp, which are instant mobile messaging applications that are used to send messages to other users of those services.

73. Subclause 4(2) clarifies that it is immaterial whether the service also enables end users to send or receive messages to or from persons other than end-users who use the carriage service.

74. Subclause 4(3) excludes carriage service providers from the scope of a message/call application service provider.

75. Subclause 4(4) excludes persons who provide billing services, or a fee collection service, in relation to a message application service, who do not provide the message application service itself.

Voice call application service

76. Clause 5 provides the definition for a voice call application service. Subclause 5(1) provides a voice call application service means any service that enables end users to make or receive voice calls to or from other end-users using a carriage service. A voice call application service is exemplified by those services currently offered by Viber or Discord.

77. Subclause 5(2) clarifies that it is immaterial whether the service also enables end users to make or receive voice calls to or from persons other than end-users who use the carriage service.

78. Subclause 5(3) excludes carriage service providers from the scope of a message/call application service provider.

79. Subclause 5(4) excludes persons who provide billing services, or a fee collection service, in relation to a voice call application service, who do not provide the voice call application service itself.
Video call application service

80. Clause 6 provides the definition for a video call application service. Subclause 6(1) provides a video call application service means any service that enables end users to make or receive video calls to or from other end-users using a carriage service. A video call application service is exemplified by those services currently offered by Skype or Facebook Messenger.

81. Subclause 6(2) clarifies that it is immaterial whether the service also enables end users to make or receive video calls to or from persons other than end-users who use the carriage service.

82. Subclause 6(3) excludes carriage service providers from the scope of a message/call application service provider.

83. Subclause 6(4) excludes persons who provide billing services, or a fee collection service, in relation to a video call application service, who do not provide the video call application service itself.

Storage/back-up service

84. Clause 7 provides the definition for a storage/back-up service. Subclause 7(1) provides a storage/back-up service means any service that enables end users to store or back-up material, where the uploading of the material for storage or back-up is by means of a carriage service. A storage/back-up service is exemplified by those services currently offered by Dropbox.

85. Subclause 7(2) excludes carriage service providers from the scope of a storage/back-up service provider.

86. Subclause 7(3) excludes persons who provide billing services, or a fee collection service, in relation to a storage/back-up service, who do not provide the storage/back up service itself.

General electronic content service

87. Clause 8 provides the definition for a general electronic content service. Subclause 8(1) provides a general electronic content service means any service that allows end users to access material using a carriage service or a service that delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service. For example, where a person provides a service that contains private or public forums that may facilitate the sharing of information or content, this would constitute a general electronic service. A general electronic content service is exemplified by those services currently offered by Facebook, Reddit and YouTube.

88. Subclause 8(2) excludes carriage service providers from the scope of a general electronic content service provider.

89. Subclause 8(3) excludes persons who provide billing services, or a fee collection service, in relation to a general electronic content service, who do not provide the general electronic content service itself.
When material is posted on a general electronic content service

90. Clause 9 describes the circumstances where material is posted on a general electronic content service. This is intended to capture scenarios such as where a person posts material on a profile page, on a social media group page, or on a chat forum, so that the material can be viewed by other users of the website or forum.

Uploaded material

91. Clause 10 describes the circumstances where a person uploads material for storage or back-up purposes. This is intended to capture scenarios where a person has uploaded electronic information for the sole purpose of storing that information, rather than with an intention to share this information with another individual.

Intended recipient of a communication

92. Clause 11 defines the intended recipient of a communication for the purposes of Schedule 1 of the TIA Act. This is modelled on section 5G of the TIA Act, but takes into account that an individual carriage service for the purposes of Schedule 1 of the TIA Act is broader than a telecommunications service.

Use of a thing

93. Clause 12 describes when a thing is used for the purposes of Schedule 1 of the TIA Act. This definition is intended to capture a broad range of uses. Clause 12 is based on clause 17 of Schedule 7 to the Broadcasting Services Act 1992, and is intended to overcome potential difficulties in attributing instrumentality to a single element of a system, where the whole system is required to perform an act.

Identification of a particular person

94. Clause 13 describes how a particular person may be identified in an IPO and includes any unique identifying factor that is applicable to the person. This definition is intentionally broad so as to capture circumstances where the real identity of the person using the account is not known.

Eligible Judge

95. Clause 14 describes how, for the purposes of this Schedule, a consenting judge may be nominated and declared by the Attorney-General to be an eligible judge. An eligible judge has the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court. Judges, in exercising their functions with respect to matters in Schedule 1 as inserted by the Bill, do so in their personal capacity.

Nominated AAT member

96. Clause 15 describes how a Deputy President, senior member or member of the AAT, as described by the clause, may be nominated by the Attorney-General to issue IPOs under Division 2 of Part 2, and Division 2 of Part 3, of this Schedule (with respect to enforcement of the criminal law, and control orders, respectively). A nomination ceases if the person’s relevant appointment to the AAT ceases. For the purposes of this Schedule, a nominated
AAT member has the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

Issuing authority

97. Clause 16 describes how the Attorney-General may, for the purposes of this Schedule, appoint as an issuing authority a judge of a court created by Parliament, or a magistrate, who has consented to the appointment. Likewise, the Attorney-General may appoint a Deputy President, senior member or member of the AAT, as described by the clause, as an issuing authority. An appointment ceases should the person cease to be a person whom the Attorney-General could appoint under this clause. An issuing authority has, for the purposes of this Schedule, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

Nominated AAT Security Division member

98. Clause 17 describes how the Attorney-General may nominate a Deputy President, senior member or member of the AAT, as described by the clause, who is also a member of the Security Division of the AAT, to issue IPOs under Part 3 of this Schedule (with respect to national security). A nomination ceases if the person’s relevant appointment to the AAT ceases, or the person ceases to be a Security Division member. A nominated AAT Security Division member has, for the purposes of this Schedule, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

Meaning of expressions in other provisions of this Act

99. Clause 18 clarifies that an expression used in Schedule 1 of the TIA Act is not intended to affect the meaning of any other expressions in the TIA Act, other than IPO or control order IPO agency.

Extra territorial application

100. Clause 19 clarifies that Schedule 1 of the TIA Act, including IPOs issued under that Schedule, has extra-territorial application.

Constitutional basis of this Schedule

101. Clause 20 establishes that Schedule 1 of the TIA Act is supported by the communications power at paragraph 51(v) of the Constitution.

102. The definition is designed to be capable of capturing a range of existing and future technologies. Examples of general electronic content services may include websites, chat forums and social media platforms.

Part 2 - International Production Orders relating to the enforcement of the criminal law

Division 1 - Simple outline

103. Clause 21 provides a simplified outline of Part 2 of Schedule 1, as introduced by the Bill.
Division 2 - International Production Orders relating to interception

Subdivision A - Applications

104. Subdivision A sets out the requirements for an interception agency to apply for an IPO relating to interception activities.

What form must an application for an International Production Order relating to interception be in?

105. Clause 22(1) provides an interception agency may apply, to an eligible Judge or nominated AAT member, for a law enforcement IPO seeking interception activities. Paragraph 22(1)(a) provides this can only be done in respect of one or more individual carriage services, or one or more individual message/call application services. This is intended to capture technologies or services associated with the making of communications by means of carriage services. For example, a message or call application service, such as Voice-over-IP services, permits persons to be able to communicate over an internet service.

106. Paragraph 22(1)(b) requires that where an interception agency makes an application to an eligible Judge or nominated AAT member, it must be directed to a designated communications provider as defined under clause 2 (definitions).

107. Subclause 22(2) requires that the interception agency nominate a designated international agreement as specified in the regulations under clause 3.

108. Subclause 22(3) provides in the case of an interception agency, members or executive officers (as described) of the particular agency may apply for an IPO.

109. Clause 23 requires that applications must be in writing unless, where urgent circumstances require an application to be made by telephone. Only the chief officer of the agency or a person who is authorised by the chief officer can make an application by telephone. Subclause 23(3) requires that any authorisation must be in writing and can be either particular persons or classes of persons.

Content of application

110. Clause 24 provides the application will state the name of the agency and the applicant.

111. Clause 25 sets out various matters to be included in the affidavit in support of an application for an IPO, including the facts or grounds on which the application is to be based.

112. Subclauses 25(3) and (4) provide that the affidavit should set out information regarding previous IPOs sought by the interception agency in relation to the same service. The inclusion of this information in the affidavit is intended to assist the eligible Judge or nominated AAT member’s consideration of the matters listed in subclauses 30(5), 39(3) and 48(5) and such as how much the information to be obtained under the IPO would likely assist in connection with the interception agency’s investigation.

113. Clause 26 provides in addition to this information, a telephone application for an IPO must include details of the urgent circumstances that led to a telephone application.
114. Clause 27 provides an eligible Judge or nominated AAT member with the power to request further information, and the form in which the further information must be given.

Submissions and questioning by the Public Interest Monitor

115. Clauses 28 and 29 allow the intervention of the Victorian and Queensland Public Interest Monitors (PIMs) to assess the applications for interception activities made by their jurisdiction’s relevant agency. Based on the information before them, the PIM may make an assessment of the application against the same criteria that the decision maker will use to make their assessment. Their assessment may then be submitted to the eligible Judge or nominated AAT member assessing the application for an IPO.

116. Under these provisions, PIMs may also question certain persons in connection with an application for an IPO. The questioning however may only take place in the presence of the eligible Judge or nominated AAT member.

117. These provisions allow the intervention of the Victorian and Queensland PIMs to assess the applications for interception activities made by their jurisdiction’s relevant agency. Nothing in this Bill is intended to prevent the PIMs from fulfilling any of their functions set out under the relevant Victorian and Queensland legislation. Rather, the Bill provides a mechanism for PIMs to monitor applications by their jurisdiction’s respective agencies for an IPO.

118. Subclauses 29(4) and 29(5) provide for the delegation by the Queensland PIM to the Queensland deputy PIM the powers under clause 29. In exercising powers under the delegation, the Queensland deputy PIM must comply with any directions of the Queensland PIM.

Subdivision B - International Production Orders relating to interception

Issue of International Production Order relating to interception – law enforcement

119. Subclause 30(1) provides an IPO relating to interception may be made in respect of one or more individual carriage services, or one or more individual message/call application services. The application must direct the order to a designated communications provider. IPOs relating to interception are limited to only those types of services recognising that these are services that permit communication via a carriage service and/or telecommunications network.

120. Subclause 30(2) provides an eligible Judge or nominated AAT member may issue an IPO if he or she is satisfied (paragraphs 30(2)(a)-(j)):

- **In the case of an application relating to one or more individual carriage services** - that there are reasonable grounds that the designated communications provider either owns or operates a telecommunications network that is, or is likely to be, used to supply the carriage services to which the order relates; or the designated communications provider supplies those individual carriage services;

- **In the case of an application concerning individual message/call application services** - that there are reasonable grounds for suspecting that the designated communications provider provides those individual message/call application services;
where the application was made by telephone, that the urgency of the situation justified a telephone application;

there are reasonable grounds for suspecting that a particular person is using, or is likely to use, those individual carriage services, or individual message/call application services;

the information to be obtained is likely to assist in connection with the investigation by the interception agency of a serious category 2 offence, or serious category 2 offences, in which the particular person is involved, or another person is involved who will be communicating with the particular person (particular person refers to the person who is involved in an offence within the meaning of section 6B of the TIA Act, whilst another person captures B-Party interception).

121. Subclause 30(2) further provides an eligible Judge or nominated AAT member may issue an order directing a designated communications provider to:

- In the case of an application in respect of one or more individual carriage services - intercept communications during a specified period, make those intercepted communications available to the interception agency, and disclose specified telecommunications data that relates to those intercepted communications and/or the services themselves.

- In the case of an application in respect of one or more individual message/call application services – intercept messages sent or received, voice calls made or received, or video calls made or received, using those services during a specified period, make those intercepted messages, voice calls or video calls available to the interception agency, and disclose specified telecommunications data that relates to those intercepted messages, voice calls or video calls, and/or the services themselves.

Period specified in the International Production Order

122. Subclause 30(3) provides an IPO must not begin in terms of interception of communications, or intercept messages sent or received, voice calls made or received, or video calls made or received before the time when the order is given to the designated communications provider. This recognises that the authority of the IPO must not permit interception activities until the IPO is given to the designated communications provider.

123. Subclause 30(3) also inserts a note which clarifies that IPOs are given under clause 111. Subclause 30(4) specifies that the period in which an IPO can require interception activities as described under subparagraphs 30(2)(i)(i) or 30(2)(j)(i) cannot be longer than 90 days, or in the case of B-Party, 45 days. The period specified in an IPO seeking B-Party interception is half that applicable to a non B-Party interception IPO, as B-Party interception inherently involves a potential for greater privacy intrusion of persons who may not be involved in the commission of an offence.

Matters to which an eligible Judge or nominated AAT member must have regard

124. Subclause 30(5) sets out a list of matters to which an eligible Judge or nominated AAT member must have regard when considering whether to issue an IPO in relation to one or more individual carriage services, or one or more individual message/call application services. An eligible Judge or nominated AAT member must have regard to the following:
• how much the privacy of any person or persons would be likely to be interfered with by intercepting communications using those services,

• the gravity of the conduct constituting the offence/offences,

• how much the information would be likely to assist in the connection with the investigation by the interception agency of the offence/offences,

• to what extent the methods of investigating the offence/offences that do not involve the interception of communications have been used by, or are available to, the interception agency,

• how much such methods would be likely to assist in connection with the investigation by the interception agency of the offence/offences,

• how much such methods would be likely to prejudice the investigation by the interception agency of the offence/offences, including whether because of delay or for any other reason,

• in relation to an application made by a Victorian interception agency – any submissions made by a Victorian PIM under clause 13 to the eligible Judge or nominated AAT member,

• in relation to an application made by a Queensland interception agency – any submissions made by a Queensland PIM under clause 14 to the eligible Judge or nominated AAT member, and

• any such other matters as the eligible Judge or nominated AAT member considers relevant (this is an additional criterion to the current domestic warrant regime under the TIA Act. It is intended to take into account the cross-border nature of the IPO regime and allow sufficient flexibility for consideration of any additional matters that may be relevant in this context).

Restriction on issuing order

125. Subclauses 30(6) and 30(7) provides an IPO relating to interception must not be issued in relation to a B-Party unless an eligible Judge or nominated AAT member are satisfied that:

• the interception agency has exhausted all other practicable methods of identifying the individual carriage services used, or likely to be used, by the person being investigated in terms of the offence/offences; or

• the interception of communications carried by individual carriage services used or likely to be used by that person would not otherwise be possible.

Content of International Production Order

126. Clause 31 sets out the content of an IPO in response to an application made by an interception agency. The order must be signed by the eligible Judge or nominated AAT member who issued the order and set out information including the name of the relevant
designated communications provider and designated international agreement, the applicable telecommunications identifiers (such as telecommunications service numbers, account holder names, or specific URLs unique to account holders), and short particulars of each serious category 2 offence or offences.

127. Subclauses 31(4), (6), and (8) provide that where an order requires the communications provider to intercept communications, messages, voice messages, voice calls or videos, or telecommunications data, the order may require the provider to do so in a specified way, and make those intercepted communications available to the interception agency in a specified way. This ensures intercepted communications are made available in a way that facilitates effective use of information provided in response to an order. For example, it may require that the designated communications provider provides the intercepted communications in a certain format to assist law enforcement in processing the intercepted communications.

128. Subclauses 31(5), (7), and (9) provide that a requirement under subclauses 31(4), (6), and (8) may include the intercepted material be made available directly to the interception agency, or require the intercepted material be made available to the interception agency indirectly via the Australian Designated Authority. This ensures maximum flexibility in the delivery of intercepted material. Interception agencies, the Australian Designated Authority, and designated communications providers have the ability to decide on an approach that achieves the goal of providing intercepted communications effectively, efficiently and in line with any designated international agreement requirements.

129. Subclause 31(10) provides the reference to specified way in clause 31 may deal with matters of timing. A note is inserted in to the subclause to provide an example requirement.

Issue of further International Production Order

130. Clause 32 establishes limitations for when a further IPO can be sought for interception activities in relation to the particular services and provider subject to an earlier IPO. A further IPO can be issued so long as the period specified in the further order begins after the end of the period specified in the original order. This is provided for both carriage services and message/call application.

131. For example, an original order specifies a period of 30 days. The interception agency may obtain a further IPO in relation to the same carriage services or message/call application services during that 30 day period, so long as the period specified on the further IPO commences after the expiry of the 30 day period specified on the original order. It is expected that an interception agency should be able to obtain sequential IPOs with no gaps between the expiry and the beginning of the new IPO to ensure that communications are not lost in transitional time.

Division 3 - International Production Orders relating to stored communications

Subdivision A - Applications

132. Subdivision A sets out the requirements for a criminal law-enforcement agency to apply for an IPO relating to stored communications.
133. Clause 33(1) provides a criminal law-enforcement agency may apply to an issuing authority for an IPO seeking stored communications. An issuing authority is defined in clause 2.

134. Applications under clause 33 must be made with respect of a particular person and directed to a designated communications provider. Therefore, an IPO may seek disclosure of an individual’s messages which were sent using a particular messaging application and emails sent to and from a specified email address.

135. Subclause 33(2) requires the application nominate a designated international agreement as specified in the regulations under clause 3.

136. Subclauses 33(3)-(4) allow for the delegation of the power to apply for an IPO under this Division.

What form must an application for an International Production Order relating to stored communications be in?

137. Clause 34 requires applications to be in writing, unless urgent circumstances require an application to be made by telephone. Only the chief officer of the agency or a person who is authorised by the chief officer can make an application by telephone. Subclause 34(3) requires that any authorisation must be in writing and can be either particular persons or classes of persons.

Content of application

138. Clause 35 provides a written application will state the name of the agency and the applicant.

139. Clause 36 provides a written application will be accompanied by one or more affidavits that set out the facts and other grounds on which the application is based.

140. Clause 37 provides in addition to this information, a telephone application for an IPO must include details of the urgent circumstances that led to a telephone application. It must also include each matter that, if the application had been made in writing, clause 35 or 36 would have required the application, or an affidavit accompanying it, to set out and must be given orally or in writing, as the issuing authority directs.

141. Clause 38 provides the issuing authority with the power to request further information in connection with the application, and the form in which the further information must be given.

Subdivision B - International Production Orders relating to stored communications

Issue of International Production Order

142. Clause 39 provides for the issuing of a law enforcement IPO relating to stored communications, by an issuing authority.

143. Subclause 39(2) sets out criteria for issuing the IPO.
144. Subclause 39(2)(a) provides the issuing authority may issue an IPO if satisfied by the information given that there are reasonable grounds for suspecting that the designated communications provider holds any of the stored communications set out in that subclause. The issuing authority has discretion to issue the order.

145. Stored communications at subclause 39(2)(a)(v) may include messages sent through a messaging application.

146. Stored communications at subclauses 39(2)(a)(vi)-(vii) may include calls made using a Voice over Internet Protocol function.

147. Stored communications at subclauses 39(2)(a)(viii) may include material on hosting services including cloud and web hosting.

148. Stored communications at subclause 39(2)(a)(ix) may include posts in a closed group page in an online social media application or in chat fora.

149. Subclause 39(2)(d) provides the issuing authority must be satisfied that the information under the order would be likely to assist in connection with the investigation by the criminal law-enforcement agency of one or more serious category 1 offence/offences involving the particular person in respect of whom the application was made. Investigation in this instance includes the prevention, detection, investigation, or prosecution of a serious crime.

150. The issuing authority may issue an order which directs the designated communications provider to do the actions set out in subclauses 39(2)(e) – (l). This includes making copies of the stored communications, making that copy available to the criminal law-enforcement agency, and to disclose specified telecommunications data.

What must the issuing authority have regard to?

151. Subclause 39(3) provides the matters to which the issuing authority must have regard in deciding whether to issue an IPO:

- how much the privacy of any person or persons would be likely to be interfered with by the criminal law-enforcement agency obtaining a copy of the stored communications,

- the gravity of the conduct constituting the offence/offences,

- how much the information would be likely to assist in connection with the investigation by the criminal law-enforcement agency of the offence/offences,

- to what extent the methods of investigating the offence/offences that do not involve obtaining a copy of the stored communications have been used by, or are available to, the criminal law-enforcement agency,

- how much such methods would be likely to assist in connection with the investigation by obtaining a copy of the stored communications of the offence/offences,
how much such methods would be likely to prejudice the investigation by obtaining a copy of the stored communications of the offence/offences, including whether because of delay or for any other reason,

any such other matters as the issuing authority considers relevant (this is an additional criterion to the current domestic warrant regime under the TIA Act. It is intended to take into account the cross-border nature of the IPO regime and allow sufficient flexibility for consideration of any additional matters that may be relevant in this context).

What must the International Production Order contain?

152. Clause 40 provides for the content of the IPO.

153. Subclause 40(2) provides the IPO must be signed by the issuing authority who issued it.

154. Subclause 40(3) provides the matters which the order must set out. This includes the name of the relevant designated communications provider and designated international agreement; and short particulars of each serious category 1 offence.

155. Subclause 40(4) provides an order may require a designated communications providers to make a copy of stored communications available to the agency in a specified way. This could include being provided in a certain format. Subclause 40(5) provides subclause 40(4) may require that a copy of stored communications be made available to the criminal law-enforcement agency directly or indirectly via the Australian Designated Authority. The intention is to allow flexibility for the Australian Designated Authority, the designated communications provider and the Australian criminal law-enforcement agency in determining how best to provide the copy of the stored communications in response to an IPO.

156. Subclauses 40(6) and 40(7) also provide for similar requirements and flexibility in terms of the disclosure of telecommunications data.

157. Subclause 40(6) provides in the case of an order that requires disclosure of telecommunications data – the order may require the provider to disclose that data in a specified way, and make that data available to the criminal law-enforcement agency in a specified way. This ensures telecommunications data is made available in a way that facilitates effective use of information provided in response to an order. For example, it may require that the designated communications provider provides the telecommunications data in a certain format to assist law enforcement in processing the telecommunications data.

158. Subclause 40(7) provides a requirement in terms of subclause 79(4) may require that the telecommunications data be made available directly to the criminal law-enforcement agency, or require that the telecommunications data is made available to the agency indirectly via the Australian Designated Authority. This ensures maximum flexibility for enforcement agencies, the Australian Designated Authority and the designated communications providers to decide on an approach that achieves the goal of providing telecommunications data effectively, efficiently and in line with any designated international agreement requirements.
159. Subclause 40(8) provides a specified way may deal with matters of timing. This could include requirements on the frequency of transmitting the data.

**Issue of further International Production Order**

160. Clause 41 enables further IPOs to be issued. Noting that a stored communications IPO is executed at a point in time (communications that are held at the time the designated communications provider receives the order), further IPOs may be required. The agency would be required to make a new application in line with the requirements of Subdivision A.

**Division 4 - International Production Orders relating to telecommunications data**

**Subdivision A - Applications**

161. Subdivision A (clauses 42 – 47) sets out general requirement provisions that apply for a valid application by an enforcement agency to an issuing authority for a telecommunications data IPO.

**What form must an application for an International Production Order relating to telecommunications data be in?**

162. Clause 42(1) sets out the circumstances in which an enforcement agency can apply for a law enforcement IPO relating to telecommunications data. The definition of enforcement agency is intended to have the same meaning given by section 176A of the TIA Act.

163. Subclause 42(2) requires that the enforcement agency nominate a designated international agreement as specified in the regulations under clause 3.

164. Subclause 42(3) provides in the case of an enforcement agency, only an authorised officer of the particular agency may apply for an IPO. The definition of authorised officer is intended to have the same meaning as that given under subsection 5(1) of the TIA Act.

165. Clause 43 requires that applications must be in writing unless urgent circumstances require an application to be made by telephone. Only the chief officer of the agency or a person who is authorised by the chief officer can make an application by telephone. Subclause 43(3) requires that any authorisation must be in writing and can be made either in relation to particular persons or classes of persons.

**Content of application**

166. Clause 44 provides the application will state the name of the agency and the applicant.

167. Clause 45 requires a written application under clause 42 for an IPO must be accompanied by an affidavit that sets out various matters to be included in support of an application for an IPO, including the facts or grounds on which the application is made. Despite subclause 45(1), a written application may be accompanied by two or more affidavits that together set out each matter that this clause, without this subclause, would have required an affidavit accompanying the application to set out.

168. Clause 46 provides in addition to this information, a telephone application for an IPO must include details of the urgent circumstances that led to a telephone application. It must also include each matter that, if the application had been made in writing, clause 42 or 43
would have required the application, or an affidavit accompanying it, to set out and must be
given orally or in writing, as the issuing authority directs.

169. Clause 47 provides an eligible Judge or nominated AAT member with the power to
request further information, and the form in which the further information must be given.

Subdivision B – International Production Orders relating to telecommunications data

170. Subdivision B (clauses 48 – 50) sets out the scope and content of a valid IPO for
telecommunications data and the general requirements that must be satisfied before an issuing
authority may issue an order to a designated communications provider.

171. Subclause 48(1) provides subclause 48 applies when an enforcement agency applies,
under clause 42, to an issuing authority for an IPO that is directed to a designated
communications provider.

172. Subclause 48(2) provides an issuing authority may issue an IPO if he or she is
satisfied that there are reasonable grounds for suspecting that the designated commu
nications provider holds, or is likely to commence to hold, any of the types of telecommunications data
listed.

173. Subclause 48(2) further provides that an issuing authority must be satisfied that:

- where the application was made by telephone, that the urgency of the situation
  justified a telephone application;

- the information to be obtained is likely to assist in connection with the investigation
  by the enforcement agency of a serious category 1 offence, or serious category 1
  offences.

174. Subclause 48(2) further provides an issuing authority may issue an order directing a
designated communications provider to:

- In the case of an application in respect of telecommunications data held by the
  designated communications provider when the IPO comes into force - disclose any
  such telecommunications data to the agency;

- In the case of an application in respect of telecommunications data held by the
  designated communications provider that commences to be held during a specified
  period - disclose any such telecommunications data to the agency.

175. Subclause 48(3) provides an IPO must not begin in terms of disclosure of
telecommunications data before the time when the order is given to the designated
communications provider. This recognises that the authority of the IPO must not permit
disclosure until the IPO is given to the designated communications provider.

176. Subclause 48(3) also inserts a note which clarifies that IPOs are given under
clause 111. Subclause 48(4) specifies that the period in which an IPO can require disclosure
as described under subclause 48(2) cannot be longer than 90 days.
177. Subclause 48(5) sets out a list of matters to which an issuing authority must have regard when considering whether to issue an IPO. Subclause 48(5)(a)-(g) sets out the list of matters which relate to one or more individual carriage services and has the following:

- how much the privacy of any person or persons would be likely to be interfered with by disclosing, under an IPO, the telecommunications data;
- the gravity of the conduct constituting the offence/offences;
- how much the information would be likely to assist in connection with the investigation by the enforcement agency of the offence/offences;
- to what extent the methods of investigating the offence/offences that do not involve the disclosure of telecommunications data have been used by, or are available to, the enforcement agency;
- how much such methods would be likely to assist in connection with the investigation by the enforcement agency of the offence/offences;
- how much such methods would be likely to prejudice the investigation by the enforcement agency of the offence/offences, including whether because of delay or for any other reason; and,
- any such other matters as the issuing authority considers relevant.

178. Clause 49 sets out the content of an IPO in response to an application made by an enforcement agency. The order must be signed by the issuing authority who issued the order and set out matters including the name of the relevant designated communications provider and designated international agreement, and short particulars of each serious category 1 offence or offences.

179. Subclause 49(4) provides in the case of an order that requires disclosure of telecommunications data – the order may require the provider to disclose that data in a specified way, and make that data available to the enforcement agency in a specified way. This ensures telecommunications data is made available in a way that facilitates effective use of information provided in response to an order. For example, it may require that the designated communications provider provides the telecommunications data in a certain format to assist law enforcement in processing the telecommunications data.

180. Subclause 49(5) provides a requirement in terms of subclause 49(4) may require that the intercepted communications be made available directly to the interception agency, or require that the telecommunications data is made available to the enforcement agency indirectly via the Australian Designated Authority. This ensures maximum flexibility for enforcement agencies, the Australian Designated Authority and the designated communications providers to decide on an approach that achieves the goal of providing telecommunications data effectively, efficiently and in line with any designated international agreement requirements.

181. Subclause 49(6) provides the reference to specified way in clause 49 may deal with matters of timing. A note is inserted in to the subclause to provide an example requirement.
182. Clause 50 sets out the limitations for when a further IPO can be sought for telecommunications data already covered by an earlier IPO. This recognises that an IPO for telecommunications data is executed at a point in time and subsequent IPOs may be required to obtain further telecommunications data.

**Part 3 - International Production Orders relating to control orders**

183. Part 3 enables control order IPO agencies to obtain an IPO for purposes in connection with a control order imposed by an issuing court under the Criminal Code. This will assist control order IPO agencies to monitor compliance with controls under a control order to protect the public from terrorist acts, prevent support for terrorist acts and hostile acts overseas and detect breaches of the control order.

**Division 1 - Introduction**

184. Clause 51 provides a simplified outline of Part 3 of Schedule 1, as introduced by the Bill.

**Division 2 - International Production Orders relating to interception**

**Subdivision A - Applications**

185. Subdivision A (clauses 52–59) sets out general requirement provisions that apply for a valid application by a control order IPO agency to an eligible Judge or nominated AAT member for an interception IPO.

**What form must an application for an International Production Order relating to interception be in?**

186. Clause 52(1) sets out where a control order IPO agency can apply for an IPO relating to interception. Subclause 52(1)(a) provides this can only be done in respect of one or more individual carriage services, or one or more individual message/call application services. This is intended to capture technologies or services associated with the making of communications by means of carriage service. For example, a message or call application service, such as Voice-over-IP services, permits persons to be able to communicate over an internet service.

187. Subclause 52(1)(b) requires that where a control order IPO agency makes an application to an eligible Judge or nominated AAT member, it must be directed to a designated communications provider as defined under clause 2 (definitions).

188. Subclause 52(2) requires that the control order IPO agency must nominate a designated international agreement as specified in the regulations under clause 3.

189. Subclause 52(3) provides, in the case of a control order IPO agency, an IPO must be applied for by certain officers, members or executive officers (as described) of the particular agency.

190. Subclause 52(4) provides the chief officer of a control order IPO agency may also nominate in writing an office or position involved in the management of the agency for this purpose.
191. Clause 53 requires that applications must be in writing, unless urgent circumstances require an application to be made by telephone. Only the chief officer of the agency or a person who is authorised by the chief officer can make an application by telephone.

192. Subclause 53(3) requires that any authorisation must be in writing and can be either particular persons or classes of persons.

Content of application

193. Clause 54 provides the application will state the name of the agency and the applicant.

194. Clause 55 provides a written application under clause 52 by a control order IPO agency for an IPO must be accompanied by an affidavit that sets out various matters to be included in support of an application for an IPO, including the facts or grounds on which the application is made.

195. Subclauses 55(3) and (4) provide that the affidavit should set out information regarding previous IPOs sought by the agency in relation to the same service. The inclusion of this information in the affidavit is intended to assist the eligible Judge or nominated AAT member’s consideration of the matters listed in subclauses 60(5) and 60(6). This aligns with similar requirements that have already been established with respect to monitoring powers currently available for control orders.

196. Clause 56 provides in addition to this information, a telephone application for an IPO must include details of the urgent circumstances that led to a telephone application. It must also include each matter that, if the application had been made in writing, clause 54 and 55 would have required the application, or an affidavit accompanying it, to set out and must be given orally or in writing, as the issuing authority directs.

197. Clause 57 provides the eligible Judge or nominated AAT member with the power to request further information, and the form in which the further information must be given.

198. Clause 58 enables the Victorian PIM to make submissions to eligible Judges or nominated AAT members or to question certain persons if a Victorian control order IPO agency applies to an eligible Judge or nominated AAT member for an IPO under clause 52.

199. Clause 59 enables the Queensland PIM to make submissions to eligible Judges or nominated AAT members or to question certain persons if a Queensland control order IPO agency applies to an eligible Judge or nominated AAT member for an IPO under clause 52.

200. Noting that both Victoria and Queensland contain legislation establishing an Office of the Public Interest Monitor, the intent of these provisions is to allow these offices the ability to consider IPOs created under the Bill. Nothing in this legislation is intended to prevent the PIMs from fulfilling any of their functions set out under the relevant legislation. Rather, the Bill provides a mechanism to give the PIMs the option of monitoring applications for IPOs.

201. In making a submission to an eligible Judge or nominated AAT member or in utilising its ability to question certain persons in relation to an order, PIMs must ensure that the matter is in relation to one or more of those set out in subclauses 60(6)(a) – (g). In questioning the person making an application for the order or a person that is providing information on the order, the eligible Judge or nominated AAT member that is intended to approve of the order must be present. This presence can be in person or via telephone.
Subdivision B - International Production Orders relating to interception

Scope and issue of International Production Orders relating to interception – control orders

202. Subclause 60(1) provides an IPO relating to interception may be made in respect of one or more individual carriage services, or one or more individual message/call application services. IPOs relating to interception are limited to only those types of services recognising that these are services that permit communication via a carriage service and/or telecommunications network. The application must direct the order to a designated communications provider.

203. Subclause 60(2) provides an eligible Judge or nominated AAT member may issue an IPO if he or she is satisfied (paragraphs 60(2)(a)-(j)):

- In the case of an application in respect of one or more individual carriage services - that there are reasonable grounds for suspecting that the designated communications provider either owns or operates a telecommunications network that is, or is likely to be, used to supply the carriage services to which the order relates; or the designated communications provider supplies those individual carriage services; and,

- In the case of an application in respect of one or more individual message/call application services - that there are reasonable grounds for suspecting that the designated communications provider provides those individual message/call application services; and,

- where the application was made by telephone, that the urgency of the situation justified a telephone application; and,

- there are reasonable grounds for suspecting that a particular person is using, or is likely to use, those individual carriage services, or individual message/call application services; and,

- In the case of an application for an International Production Order that is in respect of one or more individual carriage services:
  i. a control order is in force in relation to the particular person; or
  ii. a control order is in force in relation to another person, and the particular person is likely to communicate with the other person using those individual carriage services; and

- in the case of an application for an International Production Order that is in respect of one or more individual message/call application services:
  i. a control order is in force in relation to the particular person; or
  ii. a control order is in force in relation to another person, and the particular person is likely to communicate with the other person using those individual message/call application services; and

- in the case of an application for an IPO that is in respect of one or more individual carriage services—information that would be likely to be obtained by intercepting, under an order issued under this clause, communications that are being carried by those individual carriage services would be likely to substantially assist in connection with:
i. the protection of 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; and

• in the case of an application for an IPO that is in respect of one or more individual message/call application services—information that would be likely to be obtained by intercepting, under an order issued under this clause, messages sent or received, voice calls made or received, or video calls made or received, using those individual message/call application services would be likely to substantially assist in connection with:
  i. the protection of 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.

204. For the sake of clarity, subclause 60(2) also contains four notes to explain that the Criminal Code Act 1995 contains offences that require consideration and explains restrictions placed under subclauses 60(7) and (8).

205. Subclause 60(3) specifies that the time period for the commencement of an IPO must be after the order is given to a designated communications provider.

206. Subclause 60(3) also contains a note that explains IPOs are given under clause 111.

207. Subclause 60(4) notes that the time period specified must not be longer than 90 days for the purposes of subparagraphs 60(2)(k)(i) or (l)(i) unless subparagraphs 60(2)(g)(ii) and (h)(ii) apply, then the time period specified must not be longer than 45 days. The period specified in an IPO seeking B-Party interception is half that applicable to a non B-Party interception IPO, as B-Party interception inherently involves a potential for greater privacy intrusion of persons who may not be involved in the commission of an offence.

Matters to which the eligible Judge or nominated AAT member must have regard

208. Subclause 60(6) sets out the matters to which the eligible Judge or nominated AAT member must have regard in deciding whether to issue an IPO that is in respect of one or more individual carriage services. This subclause has been drafted to reflect the privacy considerations that are required by a Judge or nominated AAT member when issuing a domestic telecommunications interception warrant for the purpose of monitoring compliance with control orders. The matters include whether intercepting would be the method that is likely to have the least interference with any person’s privacy. This is an additional criterion to matters to which the eligible Judge or AAT member must have regard with respect to IPOs relating to interception under Part 2 or Part 3 of the Schedule. This additional consideration is
consistent with the existing control order warrant regime under the TIA Act, and provides additional protection.

209. Subclause 60(6) sets out equivalent matters to which the eligible Judge or nominated AAT member must have regard in deciding whether to issue an IPO that is in respect of one or more individual message/call application services (paragraphs 60(6)(a)-(j)). Similar to subclause 60(5), this subclause has been drafted to reflect the privacy considerations that are required by a Judge or nominated AAT member when issuing a domestic telecommunications interception warrant for the purpose of monitoring compliance with control orders and it contains similar considerations for this reason.

210. In instances where subparagraphs 60(2)(g)(ii) apply, subclause 60(7) sets out the conditions with which the eligible Judge or nominated AAT member must be satisfied before issuing an IPO:

- the requesting agency has exhausted all other practicable methods to identify the individual carriage service used, or likely to be used by the person to whom the control order relates, or
- the interception of communications carried by individual carriage services used, or likely to be used, by that person would otherwise not be possible.

211. Subclause 60(7) is intended to reduce the impact on the privacy of a person who is only in contact with someone that is subject to a control order and this is achieved by ensuring an eligible Judge or nominated AAT member has adequately turned their mind to this issue.

212. In instances where subparagraph 60(2)(h)(ii) applies, subclause 60(8) sets out the conditions that the eligible Judge or nominated AAT member must be satisfied before issuing an IPO:

- the requesting agency has exhausted all other practicable methods to identify the individual carriage service used, or likely to be used by the person to whom the control order relates, or
- the interception of messages, voice calls, video calls, or the use of individual message/call applications services used by the person or any of these that are likely to be used by the person would not otherwise be possible.

Content of International Production Order

213. Clause 61 provides for what must be included in the content of an IPO. The order must be signed by the eligible Judge or nominated AAT member who issued the order and set out details including the name of the relevant designated communications provider and designated international agreement, the applicable telecommunications identifiers (such as telecommunications service numbers, account holder names, or specific URLs unique to account holders), the name of the person, and whether the order relates to an interim or confirmed control order.

214. Subclause 61(4) provides in the case of an order that requires interception relating to communications – the order may require the provider to intercept those communications in a specified way, and make those intercepted communications available to the control order IPO agency in a specified way. This ensures intercepted communications are made available in a
way that facilitates effective use of information provided in response to an order. For example, it may require that the designated communications provider provides the intercepted communications in a specified format to assist the control order IPO agency.

215. Subclause 61(5) provides a requirement in terms of subclause 61(4) may require that the intercepted communications be made available directly to the control order IPO agency, or require that the intercepted communications be made available to the control order IPO agency indirectly via the Australian Designated Authority. This ensures maximum flexibility for a control order IPO agency, the Australian Designated Authority and the designated communications providers to decide on an approach that achieves the goal of providing intercepted communications effectively, efficiently and in line with any designated international agreement requirements.

216. Subclauses 61(6) and (7) provide the same requirements as subclauses 61(4) and (5) respectively, where it relates to an order that directs a designated communications provider to intercept messages, voice calls or video calls from a message.

217. Subclause 61(8) provides where an order directs a designated communications provider to disclose telecommunications data to the control order IPO agency, the order may require the provider to do so in a specified way. Subclause 61(9) provides an order may require that the telecommunications data be made available directly to the control order IPO agency, or require that the intercepted communications be made available to the control order IPO agency indirectly via the Australian Designated Authority.

218. Subclause 61(10) provides the reference to specified way in clause 61 may deal with matters of timing. A note is inserted into the subclause to provide an example requirement. This is to ensure that a requesting agency is given the discretion to ask for information in a way that will be able to most assist the purpose of requesting an IPO, such as receiving the information within 30 minutes in cases of urgency.

Issue of a further International Production Order

219. Clause 62 sets out the limitations for when a further IPO can be sought for interception activities already covered by an earlier IPO. A further IPO can be issued so long as the period specified in the further order begins after the end of the period specified in the original order. This is provided for both carriage services and message/call application services (subclauses (1) and (2) respectively).

220. For example, the original order has a specified period of 30 days. The control order IPO agency would be able to obtain a further IPO during that 30 days as long as the period specified would occur after the expiry of those 30 days. It is expected that the control order IPO agency should be able to obtain sequential IPOs with no gaps between the expiry and the beginning of the new IPO to ensure that communications are not missed or lost due to international time and date differences.

Division 3 - International Production Orders relating to stored communications

Subdivision A - Applications

221. Subdivision A (clauses 63 – 68) sets out general requirements that apply for a valid application by a control order IPO agency to an issuing authority for an IPO relating to stored
communications. The current domestic regime does not facilitate warrants for stored communications relating to control orders and this Bill intends to create a complimentary regime that can be applied where stored communications data is held outside Australia.

What form must an application for an International Production Order relating to stored communications be in?

222. Clause 63(1) sets out the circumstances in which a control order IPO agency can apply to an issuing authority for a law enforcement IPO relating to stored communications. An issuing authority is defined in section 5.

223. Subclause 63(1)(a) provides this can only be done in respect of a particular person. This means that IPOs are more similar to named person interception warrants than service interception warrants (consistent with the existing domestic stored communications regime under Chapter 3).

224. Subclause 63(1)(b) requires that where a control order IPO agency makes an application, it must be directed to a designated communications provider as defined under clause 2 (definitions).

225. Subclause 63(2) requires that the application nominate a designated international agreement as specified in the regulations under clause 3.

226. Subclause 63(3) sets out who can make an application on the control order IPO agency’s behalf. Similar to subclause 52(3), in the case of a control order IPO agency, an IPO must be applied for by certain officers, members or executive officers (as described) of the particular agency.

227. Subclause 63(4) provides the chief officer of a control order IPO agency may also nominate in writing an office or position involved in the management of the agency for this purpose.

228. For the purpose of complete clarity, subclause 63(5) provides subclause 63(4) is not a legislative instrument.

229. Clause 64 requires that applications must be in writing, unless urgent circumstances require an application to be made by telephone. Only the chief officer of the agency or a person who is authorised by the chief officer can make an application by telephone.

230. Subclause 64(3) requires that any authorisation must be in writing and can be either particular persons or classes of persons.

Content of application

231. Clause 65 provides a written application will state the name of the agency and the applicant. Clause 66 provides a written application will be accompanied by one or more affidavits that set out the facts and other grounds on which the application is based. Clause 67 provides in addition to this information, a telephone application for an IPO must include details of the urgent circumstances that led to a telephone application.
Clause 68 provides the issuing authority with the power to request further information in connection with the application, and the form in which the further information must be given.

**Subdivision B - International Production Orders relating to stored communications**

**Issue of an International Production Order**

Clause 69 provides for the issuing of a control order IPO relating to stored communications, by an issuing authority.

Subclause 69(1) provides an IPO relating to stored communications may be made in respect of one or more individual carriage services, or one or more individual message/call application services. Subclause 69(1)(a) provides this can only be done in respect of a particular person and subclause 69(1)(b) requires that the application must be directed to a designated communications provider as defined under clause 2 (definitions).

Subclause 69(2) sets out criteria for issuing the IPO.

Subclause 69(2)(a)-(e) specifically provides the issuing authority may issue an IPO if satisfied that:

- a control order is in force in relation to the relevant person; and
- there are reasonable grounds for suspecting that the designated communications provider holds any of the mentioned stored communications; and
- Subdivision A has been complied with in relation to the application; and
- in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
- information that would be likely to be obtained by making a copy, under an order issued under this clause, of the stored communications would be likely to substantially assist in connection with:
  1. the protection of the public from a terrorist act; or
  2. preventing the provision of support for, or the facilitation of, a terrorist act; or
  3. preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  4. determining whether the control order has been, or is being, complied with.

The issuing authority may issue an order which directs the designated communications provider to do the actions set out in subclauses 69(2)(f)-(m). This includes making copies of the stored communications, making that copy available to the control order IPO agency, and to disclose specified telecommunications data.
What must the issuing authority have regard to?

238. Subclause 69(3) provides the matters to which the issuing authority must have regard in deciding whether to issue an IPO. Having regard to these matters ensures that the issuing authority only issues an IPO in circumstances where it is justified and proportionate to do so. The list includes:

- how much the privacy of any person or persons would be likely to be interfered with by the control order IPO agency obtaining a copy of the stored communications,
- how much the information would be likely to assist in connection with:
  i. the protection of 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 has been, or is being, complied with;
- how much the use of such methods would be likely to assist in connection with the above points,
- how much such methods would be likely to prejudice the above points,
- to what extent the methods that do not involve obtaining a copy of the stored communications have been used by, or are available to, the control order IPO agency,
- any such other matters as the issuing authority considers relevant (this criterion is intended to take into account the cross-border nature of the IPO regime and allow sufficient flexibility for consideration of any additional matters that may be relevant in this context).

Content of an International Production Order

239. Clause 70 provides for the content of the IPO.

240. Subclause 70(2) sets out that the order must be signed by the eligible Judge or nominated AAT member who issued the order. Subclause 70(3) sets out that the order must set out matters including the name of the relevant designated communications provider and designated international agreement, the name of the person, and whether the order relates to an interim control order or a confirmed control order.

241. Subclause 70(4) provides an order may require a designated communications provider to make a copy of stored communications available to the agency in a specified way. This could include being provided in a certain format. Subclause 70(5) provides subclause 70(4) may require that a copy of stored communications be made available to the criminal law-enforcement agency directly or indirectly via the Australian Designated Authority. The intention is to allow flexibility for the Australian Designated Authority, the designated communications provider and the Australian law enforcement agency in determining how best to provide the copy of the stored communications in response to an IPO.
242. Subclauses 70(6) and 70(7) provide for similar requirements and flexibility in terms of the disclosure of telecommunications data.

243. Subclause 70(6) provides an IPO to direct that telecommunications data is provided in a certain way, which is to ensure any information provided in a way that is most helpful to the control order IPO agency.

244. Subclause 70(7) sets out that a requirement under 70(6) may require that the telecommunications data be disclosed to the control order IPO agency directly or indirectly via the Australian Designated Authority. Again, this subclause ensures flexibility for the benefit of a control order IPO agency requesting telecommunications data.

245. Subclause 70(8) provides a specified way may deal with matters of timing. This could include requirements on the frequency of transmitting the data.

**Issue of a further International Production Order**

246. Clause 71 enables further IPOs to be issued. Noting that a stored communications IPO is executed at a point in time (communications that are held at the time the designated communications provider receives the order), further IPOs may be required. The agency would be required to make a new application in line with the requirements of Subdivision A.

**Division 4 - International Production Orders relating to telecommunications data**

**Subdivision A - Applications**

247. Subdivision A (clauses 72–77) sets out general requirement provisions that apply for a valid application by a control order IPO agency to an issuing authority for a telecommunications data IPO.

**What form must an application for an International Production Order relating to telecommunications data be in?**

248. Clause 72(1) sets out the circumstances in which a control order IPO agency can apply for a law enforcement IPO relating to telecommunications data. The definition of control order IPO agency is intended have the meaning given by section 5 of this Bill.

249. Subclauses 72(1)(a)-(b) set out that an IPO must be issued in respect of a particular person and directed to a designated communications provider.

250. Subclause 72(2) requires that the enforcement agency nominate a designated international agreement as specified in the regulations under clause 3.

251. Subclause 72(3) provides in the case of an enforcement agency, an IPO may be applied for by an authorised officer of the particular agency. The definition of authorised officer is intended to have the same meaning as that given under subsection 5(1) of the TIA Act.

252. Clause 73 requires that applications must be in writing unless urgent circumstances require an application to be made by telephone. Only the chief officer of the agency or a person who is authorised by the chief officer can make an application by telephone.
Subclause 73(3) requires that any authorisation must be in writing and can be either particular persons or classes of persons.

**Content of application**

253. Clause 74 provides the application will state the name of the agency and the applicant.

254. Clause 75 sets out various matters to be included in the affidavit in support of an application for an IPO, including the facts or grounds on which the application is made. Despite subclause 75(1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, but for this subclause, this clause would have required an affidavit accompanying the application to set out.

255. Clause 76 provides in addition to this information, a telephone application for an IPO must include details of the urgent circumstances that led to a telephone application. It must also include each matter that, if the application had been made in writing, clause 74 or 75 would have required the application, or an affidavit accompanying it, to set out and must be given orally or in writing, as the issuing authority directs.

256. Clause 77 provides the issuing authority with the power to request further information, and the form in which the further information must be given.

**Subdivision B - International Production Orders relating to telecommunications data: control orders**

257. Subdivision B (clauses 78 – 80) sets out the scope and content of a valid IPO for telecommunications data and the general requirements that must be satisfied before an issuing authority may issue an order to a designated communications provider.

258. Subclause 78(1) provides clause 78 applies if a control order IPO agency applies to an issuing authority for an IPO that is directed to a designated communications provider.

259. Subclause 78(2)(a) provides an issuing authority may issue an IPO if he or she is satisfied a control order is in force in relation to the relevant person.

260. Subclause 78(2)(b) provides an issuing authority may issue an IPO if he or she is satisfied of the circumstances set out under paragraphs 78(2)(b)(i)–(ix) that there are reasonable grounds for suspecting that the designated communications provider holds, or is likely to commence to hold, or is likely to commence to hold, any of the types of telecommunications data listed.

261. Subclause 78(2) further provides an issuing authority must be satisfied that:

- subdivision A has been complied with in relation to the application;
- where the application was made by telephone, that the urgency of the situation justified a telephone application;
- the information to be obtained would be likely to substantially assist in connection with:
  - the protection of 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.

262. Subclause 78(2) further provides an issuing authority may issue an order directing a designated communications provider to:

- So far as the telecommunications data is held by the designated communications provider when the IPO comes into force - disclose any such telecommunications data to the agency;

- So far as the telecommunications data commences to be held by the designated communications provider during a specified period - disclose any such telecommunications data to the agency.

263. Subclause 78(3) provides an IPO must not begin in terms of disclosure of telecommunications data before the time when the order is given to the designated communications provider. This recognises that the authority of the IPO must not permit disclosure until the IPO is given to the designated communications provider.

264. Subclause 78(3) also inserts a note which clarifies that IPOs are given under clause 111. Subclause 78(4) specifies that the period in which an IPO can require disclosure as described under paragraphs 78(2)(g) cannot be longer than 90 days.

265. Subclause 78(5) sets out a list of matters to which an issuing authority must have regard when considering whether to issue an IPO. The subclause is intended to accord with the domestic approach to balancing privacy with a control order IPO agency’s need to access certain information for certain purposes. Subclause 78(5)(a)-(g) sets out the list of matters which relate to one or more individual carriage services and has the following:

- how much the privacy of any person or persons would be likely to be interfered with by the control order IPO agency obtaining a copy of the stored communications,

- how much the information would be likely to assist in connection with:
  i. the protection of 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 has been, or is being, complied with;

- how much the use of such methods would be likely to assist in connection with the above points,

- how much such methods would be likely to prejudice the above points,
to what extent the methods that do not involve obtaining a copy of the stored communications have been used by, or are available to, the control order IPO agency,

any such other matters as the issuing authority considers relevant (this criterion is intended to take into account the cross-border nature of the IPO regime and allow sufficient flexibility for consideration of any additional matters that may be relevant in this context).

266. Clause 79 provides for what must be included in the content of an IPO. The order must be signed by the issuing authority who issued the order and set out matters including the name of the relevant designated communications provider and designated international agreement, the applicable telecommunications identifiers (such as telecommunications service numbers, account holder names, or specific URLs unique to account holders), the name of the person, and whether the order relates to an interim control order or a confirmed control order.

267. Subclause 79(4) provides in the case of an order that requires disclosure of telecommunications data – the order may require the provider to disclose that data in a specified way, and make that data available to the enforcement agency in a specified way. This ensures telecommunications data is made available in a way that facilitates effective use of information provided in response to an order. For example, it may require that the designated communications provider provides the telecommunications data in a certain format to assist law enforcement in processing the telecommunications data.

268. Subclause 79(5) provides a requirement in terms of subclause 79(4) may require that the telecommunications data be made available directly to the control order IPO agency, or require that the telecommunications data is made available to the agency indirectly via the Australian Designated Authority. This ensures maximum flexibility for enforcement agencies, the Australian Designated Authority and the designated communications providers to decide on an approach that achieves the goal of providing telecommunications data effectively, efficiently and in line with any designated international agreement requirements.

269. Subclause 79(6) provides the reference to specified way in clause 79 may deal with matters of timing. A note is inserted in to the subclause to provide an example requirement.

Issue of a further International Production Order

270. Clause 80 sets out the limitations for when a further IPO can be sought for telecommunications data already covered by an earlier IPO. This recognises that an IPO for telecommunications data is executed at a point in time and subsequent IPOs may be required to obtain further telecommunications data.

Division 5 - Notification to Ombudsman by relevant agencies in relation to International Production Orders

271. Clause 81 establishes notification requirements for control order IPO agencies in relation to IPOs.

272. Subclause 81(1) sets out that, within 3 months after an IPO is issued under this Part in response to an application by a control order IPO agency, the chief officer of the agency must:
• notify the Ombudsman that the order has been issued; and
• give to the Ombudsman a copy of the order.

273. Subclause 81(2) establishes that if the chief officer of a control order IPO agency contravenes paragraph 114(1)(d) of this Schedule (so far as that paragraph relates to an IPO issued under this Part), the chief officer must:

• notify the Ombudsman of the contravention; and
• do so as soon as practicable after the contravention.

274. Subclause 81(3) ensures that a failure to comply with subclause (1) or (2) does not affect the validity of an IPO.

275. Clause 81 has been drafted to reflect section 3ZZTE of the Crimes Act 1914 and section 59B of the TIA Act as it is intended the reporting requirements that already exist for monitoring warrants are maintained under the new IPO regime.

Part 4 - International Production Orders relating to national security

Division 1 - Introduction

276. Clause 82 provides a simplified outline of Part 4 of Schedule 1, as introduced by the Bill.

Division 2 - International Production Orders relating to interception

Subdivision A - Applications

277. Clause 83 sets out where the Organisation can apply for a national security IPO relating to interception. Subclause 83(1) provides that the Organisation can apply to a nominated AAT Security Division member for an IPO in respect of one or more individual carriage services, or one or more individual message/call application services. This is intended to capture technologies or services associated with the making of communications by means of carriage services. For example, a message or call application service, such as Voice-over-IP services, which permit persons to be able to communicate over an internet service.

278. Paragraph 83(1)(b) requires that where the Organisation makes an application to a nominated AAT Security Division member, it must be directed to a designated communications provider as defined under clause 2 (definitions).

279. Subclause 83(2) requires that the Organisation nominate a designated international agreement as specified in the regulations under clause 3.

280. Subclause 83(3) provides an IPO may be applied for on the Organisation’s behalf by positions within the Organisation – namely, the Director-General of Security, or Deputy Director-General of Security, or an Organisation employee in relation to whom an authorisation is in force under subclause 83(4).
281. Subclause 83(5) provides that the Organisation can only apply to a nominated AAT Security Division member with the consent of the Attorney-General. The consent provision recognises the role of the Attorney-General as the First Law Officer and his or her ordinary role in approving intelligence collection powers of the Organisation. Whilst ordinarily these powers would not require the authorisation of a nominated AAT Security Division member, the consent by the Attorney-General, and subsequent application to the nominated AAT Security Division member is required to ensure flexibility in working with the designated international agreements.

282. Subclauses 83(6) and 83(7) set out matters regarding which the Attorney-General must be satisfied before consenting to an application being made for an IPO in respect of one or more individual carriage services, or individual message/call application services respectively, under this clause. The Attorney-General must be satisfied that:

- there are reasonable grounds for suspecting that one or more individual carriage services, or individual message/call application services, are being or likely to be:
  - used by a person engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security, or
  - the means by which the person receives or sends communications, messages etc. from or to another person who is engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security (another person captures B-Party interception); or
  - used for purposes prejudicial to security; and
- there are reasonable grounds for suspecting that the information that would be likely to be obtained by the use of the IPO communications, messages sent or received, voice calls made or received, or video calls made or received, would likely assist in the Organisation in carrying out its function of obtaining intelligence relating to security.

283. The criteria at subclauses 83(6) and 83(7) are consistent with a subset of broader criteria about which the nominated AAT member must be satisfied.

284. Subclause 83(8) requires the Attorney-General’s consent to be in writing, unless as per subclause 83(9) the person proposing to make the application considers urgent circumstances make it necessary for the Attorney-General to consent orally to the application.

285. Subclause 83(10) provides that, in the event the Attorney-General’s oral consent is given, the person must give the Attorney-General a written report setting out the urgent circumstances, and whether the application was granted, withdrawn or refused, within 3 working days of the relevant outcome. Subclause 83(11) provides that the Organisation must give the IGIS a copy of the report within the same timeframe.

What form must an application for an International Production Order relating to interception be in?

286. Clause 84 sets out the form of the application. It must be in writing unless the person applying for the IPO thinks it is necessary, because of urgent circumstances, to make the application by telephone.
**Content of application**

287. Clause 85 provides the application will state the name of the person making the application on the Organisation’s behalf and a statement to the effect that the application is made by the Organisation. In determining whether to include an Organisation employee’s name on the application, the Organisation will have due regard for any restrictions or limitations as to the name requirements under the *Australian Security Intelligence Organisation Act 1979* or other Commonwealth legislation.

288. Subclauses 86(3) and (4) provide that the affidavit should set out information regarding previous IPOs sought by the Organisation in relation to the same service. The inclusion of this information in the affidavit is intended to assist the AAT Security Division member’s consideration of the matters listed in subclauses 89(5), 98(3) and 107(5).

289. Clause 87 sets out the requirements of the information that must be given to a nominated AAT Security Division member in connection to a telephone application. The following information must be provided:

- particulars of the urgent circumstances because of which the person making the application thinks it necessary to make the application by telephone;

- each matter that, had the application been made in writing, what would have been included in that application in terms of content of the application and the accompanying affidavit; and,

- must be given in writing or orally as the nominated AAT Security Division member directs.

290. Clause 88 provides the nominated AAT Security Division member with ability to require further information, and the form in which the further information must be given.

**Subdivision B - International Production Orders relating to interception**

*Issue of an International Production Order relating to interception – national security*

291. Subclause 89(1) provides an IPO relating to interception may be made in respect of one or more individual carriage services, or one or more individual message/call application services. The application must direct the order to a designated communications provider.

292. Subclause 89(2) provides a nominated AAT Security Division member may issue an IPO if he or she is satisfied (paragraphs 89(2)(a)-(h)):

- *in the case of an application relating to one or more individual carriage services* - that there are reasonable grounds that the designated communications provider either owns or operates a telecommunications network that is, or is likely to be, used to supply the carriage services the order relates; or the designated communications provider supplies those individual carriage services;

- *In the case of an application concerning individual message/call application services* - that there are reasonable grounds for suspecting that the designated communications provider provides those individual message/call application services;
that subdivision A has been complied with in relation to the application (general application provisions and consent of Attorney-General);

where the application was made by telephone, that the urgency of the situation justified a telephone application;

there are reasonable grounds for suspecting that one or more individual carriage services, or individual message/call application services, are being or likely to be:

i. used by a person engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security, or

ii. the means by which the person receives or sends communications, messages etc. from or to another person who is engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security (another person captures B-Party interception); or

iii. used for purposes prejudicial to security.

there are reasonable grounds for suspecting that the information would be likely to be obtained by the use of the IPO communications, messages sent or received, voice calls made or received, or video calls made or received, would likely assist in the Organisation in carrying out its function of obtaining intelligence relating to security.

293. Subclause 89(2) further provides a nominated AAT Security Division member may issue an order directing a designated communications provider to:

- In the case of an application in respect of one or more individual carriage services - intercept communications during a specified period, make those intercepted communications available to the Organisation, and disclose specified telecommunications data that relates to those intercepted communications and/or the services themselves.

- In the case of an application in respect of one or more individual message/call application services – intercept messages sent or received, voice calls made or received, or video calls made or received, using those services during a specified period, and make those intercepted messages, voice calls or video calls available to the Organisation, and disclose specified telecommunications data that relates to those intercepted messages, voice calls or video calls, and/or the services themselves.

294. Clause 89 also inserts a note that clarifies that subclauses (7) and (8) restrict the issuing of IPOs if subparagraphs 89(2)(h)(ii) or (i)(ii) apply.

Period specified in the International Production Order

295. Subclause 89(3) provides an IPO must not begin in terms of interception of communications, or intercept messages sent or received, voice calls made or received, or video calls made or received before the time when the order is given to the designated communications provider. This recognises that the authority of the IPO must not permit interception activities until the IPO is given to the designated communications provider.

296. Subclause 89(4) provides the period specified in an IPO for the purposes of subparagraph (2)(i)(i) or (j)(i) must not be longer than 3 months if subparagraph 89(2)(e)(ii) or (i)(ii) applies, or 6 months otherwise. The period specified in an IPO seeking B-Party
interception is half that applicable to a non-B-Party interception IPO, as B-Party interception inherently involves a potential for greater privacy intrusion of persons who may not be involved in the commission of an offence.

*Matters to which nominated AAT Security Division member must have regard*

297. Subclause 89(5) sets out the matters to which a nominated AAT Security Division member must have regard when considering whether to issue an IPO in respect of one or more individual carriage services or individual message/call application services. Paragraphs 89(5)(a) and 89(5)(b) set out the list of matters to which the member must have regard:

- to what extent methods of carrying out the Organisation’s function of obtaining intelligence relating to security that are less intrusive than intercepting, have been used by, or are available to, the Organisation;

- how much the use of such methods would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security in so far as carrying out that function relates to the target;

- how much the use of such methods would be likely to prejudice the Organisation in carrying out this function, whether because of delay or for any other reason in so far as carrying out that function relates to the target; and,

- any such other matters as the nominated AAT Security Division member considers relevant.

298. This means that where there are other methods to access the necessary information that would be less intrusive on the privacy of the person, the Organisation may be required to turn to those means instead of seeking an IPO for interception activities.

299. While an application by the Organisation does not need to be assessed with respect to other privacy considerations, the Organisation must conduct their security intelligence activities in accordance with Ministerial Guidelines. This includes, among other things, that the Organisation’s actions should be proportionate to the gravity of the threat posed and the probability of its occurrence, and that inquiries and investigations should be done with as little intrusion into privacy as possible.

*Restriction on issuing order*

300. Subclauses 89(6)(a) and 89(6)(b) provide the nominated AAT Security Division member must not issue an IPO in a case where subparagraph 89(2)(e)(ii) applies unless the member is satisfied that the Organisation has exhausted all other practicable methods of identifying the individual carriage services or message/call application services used, or likely to be used, by the other person (i.e. the B-Party), or where the interception would not otherwise be possible. This reflects the additional privacy implications on persons not necessarily the subject of the specific investigation or intelligence activities but those that may be communicating with the person of interest.
Content of an International Production Order

301. Clause 90 sets out the content of a national security IPO relating to interception in response to an application made by the Organisation. The order must be signed by the nominated AAT Security Division member who issued the order and include matters including the name of the relevant designated communications provider and designated international agreement, and the applicable telecommunications identifiers (such as telecommunications service numbers, account holder names, or specific URLs unique to account holders).

302. Subclause 90(4) provides in the case of an order that requires interception relating to communications – the order may require the provider to intercept those communications in a specified way, and make those intercepted communications available to the Organisation in a specified way. This ensures intercepted communications are made available in a way that facilitates effective use of information provided in response to an order. For example, it may require that the designated communications provider provides the intercepted communications in a certain format to assist the Organisation in processing the intercepted communications.

303. Subclause 90(5) provides a requirement in terms of subclause 90(4) may require that the intercepted communications be made available directly to the Organisation, or require that the intercepted communications be made available to the Organisation indirectly via the Australian Designated Authority. This ensures maximum flexibility for the Organisation, the Australian Designated Authority and the designated communications providers to decide on an approach that achieves the goal of providing intercepted communications effectively, efficiently and in line with any designated international agreement requirements.

304. Subclauses 90(6) and (7) provide the same where it relates to an IPO that directs a designated communications provider to intercept messages, voice calls or video calls from a message respectively.

305. Subclause 90(8) provides where an order directs a designated communications provider to disclose telecommunications data to the Organisation, the order may require the provider to do so in a specified way. Subclause 90(9) provides an order may require that the telecommunications data be made available directly to the Organisation, or require that the intercepted communications be made available to the Organisation indirectly via the Australian Designated Authority.

306. Subclause 90(10) provides the reference to specified way in clause 90 may deal with matters of timing. A note is inserted in to the subclause to provide an example requirement.

Issue of a further International Production Order

307. Clause 91 sets out the limitations for when a further IPO can be sought for interception activities already covered by an earlier IPO. A further IPO can be issued so long as the period specified in the further order begins after the end of the period specified in the original order. This is provided for both carriage services and message/call application services (subclauses (1) and (2) respectively).

308. For example, the original order has a specified period of 30 days. The Organisation would be able to obtain a further IPO during that 30 days as long as the period specified
would occur after the expiry of those 30 days. It is expected that the Organisation should be able to obtain sequential IPOs with no gaps between the expiry and the beginning of the new IPO to ensure that communications are not missing or lost due to international time and date differences.

**Division 3 - International Production Orders relating to stored communications**

**Subdivision A - Applications**

309. Subdivision A (clauses 92 – 97) sets out general requirements that apply for a valid application by the Organisation to a nominated AAT Security Division member for an IPO relating to stored communications.

310. Clause 92 sets out where the Organisation can apply for a national security IPO relating to interception. Subclause 92(1)(a) provides that the Organisation can apply to a nominated AAT Security Division member for an IPO in respect of a particular person. This means that IPOs are more similar to named person interception warrants than service interception warrants (consistent with the existing domestic stored communications regime under Chapter 3). For example, an IPO may authorise access to all messages associated with a single messaging application and all emails sent to and from a specified email address.

311. Subclause 92(1)(b) requires the IPO be directed to a *designated communications provider* as defined under clause 2 (definitions).

312. Subclause 92(2) requires that an application must nominate a designated international agreement.

313. Subclause 92(3) provides an IPO may be applied for by positions within the Organisation – namely, the Director-General of Security, or Deputy Director-General of Security, or an Organisation employee in relation to whom an authorisation is in force under subclause 92(4).

314. Subclause 92(5) provides that the Organisation can only apply to a nominated AAT Security Division member with the consent of the Attorney-General. The consent provision recognises the role of the Attorney-General as the First Law Officer and his or her ordinary role in approving intelligence collection powers of the Organisation. Whilst ordinarily these powers would not require the authorisation of a nominated AAT Security Division member, the consent by the Attorney-General, and subsequent application to the nominated AAT Security Division member is required to ensure flexibility in working with the designated international agreements.

315. Subclause 92(6) provides the Attorney-General must not consent to the making of the application unless satisfied that:

- there are reasonable grounds for suspecting that the person is engaged in, or is likely to engage in, activities prejudicial to security; and

- information that would be likely to be obtained would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security.

316. The criteria at subclause 92(6) are consistent with a subset of broader criteria about which the nominated AAT member must be satisfied.
317. Subclause 92(7) requires the Attorney-General’s consent to be in writing, unless as per subclause 92(8) the person proposing to make the application considers urgent circumstances make it necessary for the Attorney-General to consent orally to the application.

318. Subclause 92(9) provides that, in the event the Attorney-General’s oral consent is given, the person must give the Attorney-General a written report setting out the urgent circumstances, and whether the application was granted, withdrawn or refused, within 3 working days of the relevant outcome. Subclause 92(10) provides that the Organisation must give the IGIS a copy of the report within the same timeframe.

**What form must an application for an International Production Order relating to stored communications be in?**

319. Clause 93 requires that applications must be in writing, unless urgent circumstances require an application to be made by telephone. An application by telephone must only be made where the person making the application thinks it necessary, because of urgent circumstances, to make the application by telephone. Urgent circumstances could include, for example, potential loss of intelligence, loss of life or serious damage to property.

**Content of application**

320. Clause 94 provides a written application will state the name of the Organisation and the applicant. Clause 95 provides a written application will be accompanied by one or more affidavits that set out the facts and other grounds on which the application is based. Clause 96 provides in addition to this information, a telephone application for an IPO must include details of the urgent circumstances that led to a telephone application.

321. Clause 97 provides the nominated AAT Security Division member with the ability to require further information in connection with the application, and the form in which the further information must be given.

**Subdivision B - International Production Orders relating to stored communications**

322. Clause 98 provides for the issuing of a national security IPO relating to stored communications, by a nominated AAT Security Division member. Subclause 98(1) sets out that an IPO applies in respect of a particular person and must be directed to a designated communications provider.

323. Subclause 98(2) sets out the criteria for issuing the IPO. Subclause 98(2) provides the nominated AAT Security Division member may issue an IPO if satisfied by the information given that:

- there are reasonable grounds for suspecting that the relevant person is engaged in, or is likely to engage in, activities prejudicial to security,
- there are reasonable grounds for suspecting that the designated communications provider holds any of the stipulated stored communications,
- Subdivision A has been complied with (general application provisions and the consent of the Attorney-General),
in the case of a telephone application – because of urgent circumstances, it was necessary to make the application by telephone, and

the information that would be likely to be obtained by making a copy of the stored communications would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security.

324. The nominated AAT Security Division member may issue an order which directs the designated communications provider to do the actions set out in subclauses 98(2)(f) – (m). This includes making copies of the stored communications, making that copy available to the Organisation, and to disclose specified telecommunications data.

Matters to which nominated AAT Security Division member must have regard

325. Subclause 98(3) provides the matters to which the nominated AAT Security Division member must have regard in deciding whether to issue an IPO relating to stored communications. The member is required have regard to:

- to what extent methods of carrying out the Organisation’s function of obtaining intelligence relating to security that are less intrusive have been used by, or are available to, the Organisation;
- how much the use of such methods would be likely to assist the Organisation in carrying out its function of obtaining intelligence relating to security in relation to the specific purposes of the IPO;
- such other matters (if any) as the nominated AAT Security Division member considers relevant.

What must the International Production Order contain?

326. Clause 99 sets out what must be contained in the IPO. The IPO must be signed by the nominated AAT Security Division member who issued it.

327. Subclauses 99(3) – (8) set out specific requirements, including that the order must set out the date on which the order was issued, the name of the designated communications provider, and the name of the designated international agreement.

328. Subclause 99(4) provides an order may require a designated communications provider to make a copy of stored communications available to the Organisation in a specified way. This could include being provided in a certain format. Subclause 99(5) provides subclause 99(4) may require that a copy of stored communications be made available to the Organisation directly or indirectly via the Australian Designated Authority. The intention is to allow flexibility for the Australian Designated Authority, the designated communications provider and the Organisation in determining how best to provide the copy of the stored communications in response to an IPO.

329. Subclauses 99(6) and 99(7) provide for similar requirements and flexibility in terms of the disclosure of telecommunications data.

330. Subclause 99(8) provides a specified way may deal with matters of timing. This could include requirements on the frequency of transmitting the data.
Issue of further International Production Order

331. Clause 100 provides for a further IPO for stored communications in respect of a person, or directed to a designated communications provider. Noting that a stored communications IPO is executed at a point in time (communications that are held at the time the designated communications provider receives the order), further IPOs may be required. The Organisation would be required to make a new application in line with the requirements of Subdivision A.

Division 4 - International Production Orders relating to telecommunications data

Subdivision A - Applications

332. Subdivision A (clauses 101 – 106) sets out general requirements that apply for a valid application by the Organisation to a nominated AAT Security Division member for an IPO relating to telecommunications data.

333. Subclause 101(1) sets out where the Organisation can apply to a nominated AAT Security Division member for an IPO relating to telecommunications data.

334. Paragraph 101(1)(a) provides this can only be done in respect of a particular person. This means that IPOs are more similar to named person interception warrants than service interception warrants.

335. Paragraph 101(1)(b) requires that where the Organisation makes an application, it must be directed to a designated communications provider as defined under clause 2 (definitions).

336. Subclause 101(2) requires that an application must nominate a designated international agreement.

337. Subclause 101(3) provides an IPO may be applied by positions within the Organisation – namely, the Director-General of Security, or Deputy Director-General of Security, or an Organisation employee in relation to whom an authorisation is in force under subclause 101(4).

What form must an application for an International Production Order relating to telecommunications data be in?

338. Clause 102 requires that applications must be in writing, unless urgent circumstances require an application to be made by telephone. An application by telephone must only be made where the person making the application thinks it necessary, because of urgent circumstances, to make the application by telephone. Urgent circumstances could include, for example, potential loss of intelligence, loss of life or serious damage to property.

Content of application

339. Clause 103 provides a written application will state the name of the Organisation and the applicant. Clause 104 provides a written application will be accompanied by one or more affidavits that set out the facts and other grounds on which the application is based. Clause 105 provides in addition to this information, a telephone application for an IPO must include details of the urgent circumstances that led to a telephone application.
Clause 106 provides the nominated AAT Security Division member with the ability to require further information in connection with the application, and the manner in which it must be given.

Subdivision B - International Production Orders relating to telecommunications data

Subdivision B (clauses 107 to 109) sets out the scope and content of a valid IPO for telecommunications data and the general requirements that must be satisfied before an nominated AAT Security Division member may issue an order.

Subclause 107(1) sets out the scope of an IPO when the Organisation applies for an IPO for telecommunications data to a nominated AAT Security Division member.

Subclause 107(1)(a) provides this can only be done in respect of a particular person. Subclause 107(1)(b) requires that the application must be directed to a designated communications provider as defined under clause 2 (definitions).

Subclause 107(2) provides a nominated AAT Security Division member may issue an IPO if he or she is satisfied of the following:

- there are reasonable grounds for suspecting that the designated communications provider holds, or is likely to commence to hold any of the following telecommunications data:
  
  i. telecommunications data that relates to the communications the relevant person has made using an individual carriage service supplied by the designated communications providers;

  *For example, the internet identifier (information that uniquely identifies a person on the Internet) assigned to the user by the provider*

  ii. telecommunications data that relates to an individual carriage service supplied using a telecommunications network owned or operated by the designated communications provider, where the individual carriage service is used, or likely to be used, by the relevant person;

  *For example, the number called or texted for a mobile service.*

  iii. telecommunications data that relates to an individual carriage service supplied by the designated communications provider, where the individual carriage service is used, or is likely to be used, by the relevant person;

  *For example, billing and account information for an internet account.*

  iv. telecommunications data that relates to messages sent or received by the relevant person using an individual message/call application service provided by the designated communications provider;

  *For example, the destination account that a message was sent to on an instant messaging mobile application.*
v. telecommunications data that relates to voice calls made or received by the relevant person using an individual message/call application service provided by the designated communications provider;

For example, details of voice calls made or received by a particular telecommunications application account.

vi. telecommunications data that relates to video calls made or received by the relevant person using an individual message/call application service provided by the designated communications provider;

For example, details of video calls made or received by a particular video chat account.

vii. telecommunications data that relates to an individual message/call application service provided by the designated communications provider, where the individual message/call application service is used, or is likely to be used, by the relevant person;

For example, account information for an instant messaging account.

viii. telecommunications data that relates to material that has been uploaded by the relevant person for storage or back up by a storage/back up service provided by the designated communications provider that there are reasonable grounds for suspecting that the designated communications provider holds, or is likely to commence to hold, telecommunications data that relates;

For example, the date and time in which material was uploaded to a cloud storage service.

ix. telecommunications data that relates to material that has been posted by the relevant person on a general electronic content service provided by the designated communications provider.

For example, the Internet Protocol address associated with a particular post in a chat forum.

- Subdivision A has been complied with in relation to the provisions of general application;

- in the case of a telephone application – that it was necessary due to urgent circumstances;

- disclosure of the telecommunications data would be in connection with the performance by the Organisation of its functions.

345. Subclause 107(2) further provides a nominated AAT Security Division member may issue an order directing the designated communications provider to:

- In the case of an application in respect of telecommunications data is held by the designated communications provider when the International Production Order comes into force - disclose any such telecommunications data to the Organisation;
In the case of an application in respect of telecommunications data commences to be held by the designated communications provider commences to be held during a specified period - disclose any such telecommunications data to the Organisation.

346. Subclause 107(3) provides an IPO must not begin in terms of disclosure of telecommunications data before the time when the order is given to the designated communications provider. This recognises that the authority of the IPO must not permit disclosure until the IPO is given to the designated communications provider.

347. Subclause 107(4) specifies that the period in which an IPO can require disclosure as described under paragraphs 107(2)(f) cannot be longer than 90 days. This is consistent with the period for an authorisation for access to prospective telecommunications data under the existing TIA Act.

348. Subclause 107(5) provides the matters to which the nominated AAT Security Division member must have regard in deciding whether to issue an IPO relating to telecommunications data. The member is required have regard to:

- to what extent methods of carrying out the Organisation’s function of obtaining intelligence relating to security that are less intrusive have been used by, or are available to, the Organisation
- how much the use of such methods would be likely to assist the Organisation in carrying out its functions in relation to the specific purposes of the IPO in so far as carrying out that function relates to the target.
- how much the use of such methods would be likely to prejudice the Organisation in carrying out its functions, whether because of delay or for any other reason in so far as carrying out that function relates to the target.
- such other matters (if any) as the nominated AAT Security Division member considers relevant.

What must the International Production Order contain?

349. Clause 108 sets out the content of an IPO in response to an application made by the Organisation. The order must be signed by the nominated AAT Security Division member who issued the order and set out the date on which the order was issued, the name of the relevant designated communications provider and the name of designated international agreement.

350. Subclause 108(4) provides in the case of an order that requires disclosure of telecommunications data – the order may require the provider to disclose that data in a specified way, and make that data available to the Organisation in a specified way. This ensures telecommunications data is made available in a way that facilitates effective use of information provided in response to an order. For example, it may require that the designated communications provider provides the telecommunications data in a certain format to assist law enforcement in processing the telecommunications data.

351. Subclause 108(5) provides a requirement in terms of subclause 108(4) may require that the intercepted communications be made available directly to the interception agency, or
require that the telecommunications data is made available to the Organisation indirectly via the Australian Designated Authority. This ensures maximum flexibility for the Organisation, the Australian Designated Authority and the designated communications providers to decide on an approach that achieves the goal of providing telecommunications data effectively, efficiently and in line with any designated international agreement requirements.

352. Subclause 108(6) provides the reference to specified way in clause 108 may deal with matters of timing. A note is inserted in to the subclause to provide an example requirement.

353. Clause 109 provides for a further IPO for telecommunications data in respect of a particular person and directed to a designated communications provider. This recognises that an IPO for telecommunications data is executed at a point in time and subsequent IPOs may be required to obtain further telecommunications data. The Organisation would be required to make a new application in line with the requirements of Subdivision A.

**Part 5 - Giving of International Production Orders**

354. Clause 110 provides a simplified outline of Part 5 of Schedule 1, as introduced by the Bill.

*Provision of International Production Orders to Australian Designated Authority—relevant agency*

355. Subclause 111(1)(a) provides if an IPO is issued under Part 2 or 3 of the Schedule then the relevant agency that obtained the IPO must give the IPO, or a certified copy of the IPO, to the Australian Designated Authority. In practice, the IPO or certified copy of the IPO may be provided electronically, including through a technical system established between the relevant agency and the Australian Designated Authority.

*Review of International Production Orders—relevant agency*

356. Subclause 111(1)(b) requires the Australian Designated Authority to consider whether the IPO complies with the designated international agreement nominated in the application for the order. In reviewing an order for compliance with the designated international agreement, the Australian Designated Authority will consider the order against any limitations or restrictions specified in the designated international agreement with the relevant country, such as any limitations on what criminal offences orders can relate to, who may be targeted by an order, what types of data can be sought under an order, and what communications providers an order may be directed to.

357. This review may need to be more detailed, or more cursory, depending on the complexity of the order, and the complexity of the nominated designated international agreement. This review process by the Australian Designated Authority will help to ensure that each designated international agreement is applied in relation to each order that is given pursuant to that particular designated international agreement.

358. Subclause 111(1)(c) provides, if the Australian Designated Authority is satisfied that an IPO complies with the nominated designated international agreement, then the Australian Designated Authority must give the order or a certified copy of the order to the designated communications provider to which the order is directed as soon as practicable. In practice, it is anticipated that the time it takes for the Australian Designated Authority to give an order could be affected by whether or not the designated communications provider has provided an
electronic address for service and the technical capability of designated communications providers to receive orders electronically, including through a technical system established between the Australian Designated Authority and the designated communications provider.

359. Subclause 111(1)(d) provides, if the Australian Designated Authority is not satisfied that an IPO complies with the nominated designated international agreement, then the Australian Designated Authority must cancel the IPO and return the IPO, or the certified copy of the IPO, to the relevant agency that obtained the IPO. In practice, the IPO, or certified copy of the IPO, may be returned to the relevant agency electronically or through a notification to the relevant agency sent via a technical system established between the relevant agency and the Australian Designated Authority.

360. Subclause 111(1)(d)(iii) provides where the Australian Designated Authority cancels an IPO, it must also provide such advice as the Australian Designated Authority considers appropriate to the relevant agency that obtained the IPO in relation to compliance with the designated international agreement nominated in the IPO.

361. The Australian Designated Authority may choose to provide its advice to the relevant agency at the same time the IPO is returned to the agency, or afterwards. The length, nature and content of this advice is at the discretion of the Australian Designated Authority, and may be determined on a case-by-case basis. In practice, the advice may include advice on the aspects of the IPO that are considered to be inconsistent with the nominated designated international agreement.

362. Subclause 111(2) provides, if the Australian Designated Authority gives a certified copy of an IPO to a designated communications provider, then the Australian Designated Authority is taken to have given the IPO to the designated communications provider under subclause 111(1). In practice, designated communications providers will generally be based in foreign countries and correspondence with designated communications providers, including the giving of IPOs, will generally be done electronically. Ensuring that a certified copy of an IPO can be given to a designated communications provider will also streamline the time it takes for an IPO to be given and responded to.

When an International Production Order comes into force—relevant agency

363. Subclause 111(3) provides an IPO does not come into force until the Australian Designated Authority gives the order to the designated communications provider to which it is directed. This means that the order does not place any legal obligations on the designated communications provider under the Schedule until the order has been given to them.

364. Subclause 111(4) provides an order is taken to invoke the designated international agreement nominated in the order at the time it is given to the designated communications provider under subclause 111(1). This means that the order does not place any obligations on the designated communications provider pursuant to the nominated designated international agreement until the order has been given to them.

Notification of giving of International Production Orders—relevant agency

365. Subclause 111(5) provides, if the Australian Designated Authority gives an order to a designated communications provider, then it must also notify the relevant agency that
obtained the order that the order has been given. This notification may be made at the same
time the order is given to the designated communications provider, or afterwards.

366. Subclause 111(6) provides a cancellation under subclause 111(1) must be set out by
the Australian Designated Authority in a written instrument.

367. Subclause 111(7) provides that the relevant agency that applied for the order may give
further information to the Australian Designated Authority to assist the Australian Designated
Authority in making a decision under this clause. This is intended to enable the relevant
agency to provide additional information to the Australian Designated Authority that relates
to the order’s compliance with requirements of the designated international agreement.

Provision of International Production Order to Australian Designated Authority—
Organisation

368. Subclause 112(1)(a) provides if an order is issued under Part 4 of the Schedule then
the Organisation must give the order, or a certified copy of the order, to the Australian
Designated Authority. In practice, the order or certified copy of the order may be provided
electronically, including through a technical system established between the Australian
Designated Authority and the Organisation.

Review of International Production Orders—Organisation

369. Subclause 112(1)(b) requires the Australian Designated Authority to consider whether
the IPO complies with the designated international agreement nominated in the application
for the order. In the reviewing an order for compliance with the designated international
agreement, the Australian Designated Authority will consider the order against any
limitations or restrictions specified in the designated international agreement with the
relevant country, such as any limitations on what criminal offences orders can relate to, who
may be targeted by an order, what types of data can be sought under an order, and what
communications providers an order may be directed to. This review may need to be more
detailed, or more cursory, depending on the complexity of the order, and the complexity of
the nominated designated international agreement.

370. This review process by the Australian Designated Authority will help to ensure that
each designated international agreement is consistently applied in relation to each order that
is given pursuant that designated international agreement.

371. Subclause 112(1)(c) provides, if the Australian Designated Authority is satisfied that
an order complies with the nominated designated international agreement, then the Australian
Designated Authority must give the order or a certified copy of the order to the designated
communications provider to which the order is directed as soon as practicable. In practice, it
is anticipated that the time it takes for the Australian Designated Authority to give an order
could be affected by whether or not the designated communications provider has provided an
electronic address for service and the technical capability of designated communications
providers to receive orders electronically, including through a technical system established
between the Australian Designated Authority and the designated communications provider.

372. Subclause 112(1)(d) provides, if the Australian Designated Authority is not satisfied
that an order complies with the nominated designated international agreement, then the
Australian Designated Authority must cancel the order and return the order, or the certified
copy of the order, to the Organisation. In practice, the order, or certified copy of the order, may be returned to the Organisation electronically or through a notification sent via a technical system established between the Australian Designated Authority and the Organisation.

373. Subclause 112(1)(d)(iii) provides, where the Australian Designated Authority cancels an order, it must also provide such advice to the Organisation as the Australian Designated Authority considers appropriate in relation to compliance with the designated international agreement nominated in the order.

374. The Australian Designated Authority may choose to provide its advice to the Organisation at the same time the order is returned to the agency, or afterwards. The length, nature and content of this advice is at the discretion of the Australian Designated Authority, and may be determined on a case-by-case basis. In practice, the advice may include advice on the aspects of the order that are considered to be inconsistent with the nominated designated international agreement.

375. Subclause 112(2) provides, if the Australian Designated Authority gives a certified copy of an order to a designated communications provider, then the Australian Designated Authority is taken to have given the order to the designated communications provider under subclause 112(1). In practice, designated communications providers will generally be based in foreign countries and correspondence with designated communications providers, including the giving of orders, will generally be done electronically. Ensuring that a certified copy of an order can be given to a designated communications provider will also streamline the time it takes for an order to be given and responded to.

When an International Production Order comes into force—Organisation

376. Subclause 112(3) provides an order does not come into force until the Australian Designated Authority gives the order to the designated communications provider to which it is directed. This means that the order does not place any legal obligations on the designated communications provider under the Schedule until the order has been given to them.

377. Subclause 112(4) provides an order is taken to invoke the designated international agreement nominated in the order at the time it is given to the designated communications provider under subclause 112(1). This means that the order does not place any obligations on the designated communications provider pursuant to the nominated designated international agreement until the order has been given to them.

Notification of giving of International Production Orders—Organisation

378. Subclause 112(5) provides, if the Australian Designated Authority gives an order to a designated communications provider, then it must also notify the Organisation that the order has been given. This notification may be made at the same time the order is given to the designated communications provider, or afterwards.

379. Subclause 112(6) provides a cancellation under subclause 112(1) must be set out by the Australian Designated Authority in a written instrument.
Subclause 112(7) provides that the Organisation may give further information to the Australian Designated Authority to assist the Australian Designated Authority in making a decision under this clause. This is intended to enable the Organisation to provide additional information to the Australian Designated Authority that relates to the order’s compliance with requirements of the designated international agreement.

**Part 6 - Revocation of International Production Orders**

381. Clause 113 provides a simplified outline of Part 6 of Schedule 1, as introduced by the Bill.

**Revocation of International Production Orders—relevant agency**

382. Clause 114 provides for revocation of IPOs by the relevant agency.

383. Subclause 114(1) is with respect to IPOs issued under Part 2, or Part 3, of the Schedule, which relates to enforcement of the criminal law or control orders respectively. If the IPO is in force, and it was issued in response to an application made by a relevant agency, then the chief officer of the agency may revoke the order. The chief officer must revoke the order if satisfied that the grounds on which the order was issued have ceased to exist. This mechanism is designed to avoid any doubt on the status of an IPO when the grounds for issuing an order are no longer valid. Beyond ensuring privacy is relevantly protected in these circumstances, the provision will also allow for more accurate reporting of IPOs.

384. Subclause 114(2) requires that a revocation under this provision be set out in a written instrument.

**Giving of instrument of revocation—relevant agency**

385. Clause 115 sets out the requirements for the giving of an instrument of revocation by a relevant agency.

386. Subclause 115(1) provides if an IPO is revoked pursuant to clause 114 the relevant agency must give the instrument of revocation to the Australian Designated Authority, and do so as soon as practicable after the order is revoked. The Australian Designated Authority must give the instrument of revocation to the designated communications provider to whom the order is directed, and do so as soon as practicable after it has received the instrument of revocation. This will ensure a provider that is issued an IPO that is subsequently revoked becomes aware of the revocation and cease transmitting any relevant electronic information.

387. Subclause 115(3) provides the revocation takes effect when the instrument of revocation is given to the designated communications provider.

**Revocation of International Production Orders—Organisation**

388. Clause 116 provides for revocation of IPOs issued to the Organisation.

389. Subclause 116(1) is with respect to IPOs issued under Part 4 of Schedule 1 of the TIA Act, which relate to national security. If the IPO is in force, then the Director-General of Security may revoke the order. The Director-General of Security must revoke the order if satisfied that the grounds on which the order was issued have ceased to exist.
390. Subclause 116(2) requires that a revocation under this provision be set out in written instrument.

Giving of instrument of revocation—Organisation

391. Subclause 117 sets out the requirements for the giving of an instrument of revocation by the Organisation.

392. Subclause 117(1) requires that if an IPO is revoked pursuant to clause 116 by the Director-General of Security the Organisation must give the instrument of revocation to the Australian Designated Authority, and do so as soon as practicable after the order is revoked.

393. Subclause 117(2) requires that the Australian Designated Authority must give the instrument of revocation to the designated communications provider to whom the order is directed, and do so as soon as practicable after it has received the instrument of revocation.

394. Subclause 117(3) provides the revocation takes effect when the instrument of revocation is given to the designated communications provider.

Delegation by the chief officer of a relevant agency

395. Subclause 118(1) provides the chief officer of a relevant agency may delegate any or all powers under this Part to a certifying officer of the agency. Subclause 118(2) provides the delegate must comply with any directions of the chief officer when performing functions, or exercising powers under a delegation under subclause 118(1).

Delegation by the Director-General of Security

396. Subclause 119(1) provides the Director-General of Security may delegate any or all powers under this Part to a Deputy Director-General of Security or an Organisation employee. Subclause 119(2) provides the delegate must comply with any directions of the Director-General of Security when performing functions, or exercising powers under a delegation under subclause 119(1).

397. The purpose of the delegation powers at subclauses 118 and 119 is to enable appropriate persons to perform functions or powers related to revocation of IPOs, streamlining processes in order to assist the relevant agency or the Organisation to discharge its functions.

Part 7 - Objections to, and cancellation of, International Production Orders

398. Clause 120 provides a simplified outline of Part 7 of Schedule 1, as introduced by the Bill.

Objections by designated communications providers

399. Clause 121 provides a designated communications provider may object to an IPO.

400. Subclause 121(1) provides the designated communications provider to which an IPO is directed may, by written notice given to the Australian Designated Authority, object to the order on the grounds that, in the view of the designated communications provider, the order does not comply with the designated international agreement nominated in the application for
the order. For example, if the provisions of the designated international agreement place restrictions on the types of providers that Australian orders can be issued to, and the provider considers it is not a provider covered under the agreement, then it could raise an objection on that basis.

401. Subclause 121(2) requires that the written notice must be given to the Australian Designated Authority within a reasonable time after the IPO is given to the designated communications provider. The written notice must also set out the reasons why the provider considers that the order does not comply with the nominated designated international agreement.

402. The ability of a designated communications provider to object to an IPO under clause 120 is in addition to any other judicial, administrative or other review rights or remedies that may be available to the provider under Australian law.

*Cancellation of International Production Orders*

403. Clause 122 provides for the cancellation of an IPO by the Australian Designated Authority.

404. Subclause 122(1) provides the Australian Designated Authority may cancel an IPO, including prior to or after giving it to a designated communications provider. In practice, the Australian Designated Authority may decide to cancel an order for a range of reasons including, for example, because the Australian Designated Authority considers it is in the public interest to do so, or following dispute resolution with the designated communications provider or the government of a foreign country. Upon cancellation, the IPO will cease to be in force.

405. Subclause 122(2) provides a cancellation under subclause 122(1) must be set out in a written instrument.

406. Subclause 122(3) provides, if an IPO is cancelled under subclause 122(1), and the order was issued under Part 2 or Part 3 in response to an application by a relevant agency, the Australian Designated Authority must inform the chief officer of the relevant agency as soon as practicable after cancelling the order. If an IPO is cancelled under subclause 122(1), and the IPO was issued under Part 4, the Australian Designated Authority must inform the Organisation of the cancellation as soon as practicable after the cancelling the order.

407. Subclause 122(4) provides, if the Australian Designated Authority gave an IPO to the designated communications provider to whom the order is directed, and the order was subsequently cancelled pursuant to subclause 122(1), the Australian Designated Authority must give the instrument of cancellation to the designated communications provider as soon as practicable after cancelling the order.

408. Subclause 122(5) provides, if the instrument of cancellation is required to be given to the designated communications provider, then a cancellation under subclause 122(1) takes effect when the instrument is given. This is intended to ensure the designated communications provider is aware of the cancellation and can cease complying with the order. Otherwise, the cancellation takes effect from when it is made.
Part 8 - Compliance with International Production Orders

409. Part 8 establishes a framework for compliance with IPOs.

410. Clause 123 provides a simplified outline of Part 8 of Schedule 1, as introduced by the Bill.

411. Clause 124 provides, if an IPO is given to the designated communications provider to whom it is directed, and is in force, and the designated communications provider meets the enforcement threshold, the designated communications provider must comply with the order to the extent that it is capable of doing so. The item provides failure to do so attracts a civil penalty of 238 penalty units. Non-compliance with an IPO may jeopardise law enforcement or national security objectives, including resulting in the destruction of material evidence. Accordingly, the penalty is appropriate to achieve the primary aim of deterrence from non-compliance. An IPO will not be considered in force if it has been revoked or cancelled.

The enforcement threshold

412. The enforcement threshold requires a certain connection between the designated communications provider’s service and Australia. While IPOs can be issued broadly to all designated communications providers, it is appropriate that the compliance framework attach an enforcement threshold in order to ensure its practical effectiveness.

413. Clause 125 identifies when a designated communications provider meets the enforcement threshold referenced in paragraph 124(c). For the purposes of Schedule 1, subclause 125(1) provides that if a designated communications provider supplies a service to one or more Australians, or owns or operates a telecommunications network that is used to supply a carriage service to one or more Australians, or one or more Australians have posted material on a general electronic content service provided by a designated communications provider, the provider meets the enforcement threshold, unless the provider cannot reasonably be considered to have offered or provided the service on the basis of the service being available to Australians, or if the provider cannot reasonably be considered to have offered or provided the general electronic content service on the basis of the opportunity to post material on the service being available to Australians.

414. Paragraphs (a)-(j) set out the specific criteria for each of the designated communications providers defined in Part 1. A reference to one or more Australians does not need to mean the person to which the order relates, or any other specific person.

415. This provision sets out a two-part test for the compliance framework to apply. Firstly, the ‘minimum contacts’ test that requires there be a minimum of one or more Australians using the service, who are ordinarily resident in Australia. The second part sets out when a designated communications provider does not meet the threshold, on an exception basis. The second part is a ‘reasonableness’ test that goes to whether the designated communications provider could not reasonably be considered to have offered or provided the service to Australians at the time the order was given. The intention is to permit legal process to be served on a wide array of providers, but to exclude from the compliance framework local services that restrict their services to particular local identifiers for access, or passive services that have no intention that Australians use their services.
416. Subclause 125(2) provides Australian means an individual who is ordinarily resident in Australia. This is consistent with the definition in the Enhancing Online Safety Act 2015. Subclause 125(3) identifies an end-user as including a prospective end-user.

**Enforceable civil penalty provision**

417. Subclause 126(1) provides a civil penalty provision in Part 8 of Schedule 1, as introduced by the Bill, is enforceable under Part 4 of the Regulatory Powers (Standard Provision) Act 2014 (RPA Act). The item also includes a note to the effect that Part 4 of the RPA Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

**Authorised applicant**

418. Subclause 126(2) provides, for the purposes of Part 4 of the RPA Act, the Communications Access Co-ordinator is an authorised applicant in relation to a civil penalty provision in Part 8 of Schedule 1. Communications Access Co-ordinator is an independent officer within the Department of Home Affairs and is further defined in section 6R of the TIA Act.

**Relevant court**

419. Subclause 126(3) provides, for the purposes of Part 4 of the RPA Act, the Federal Court of Australia and the Federal Circuit Court of Australia are the relevant courts with respect to any proceedings under this Part.

**Penalty for a body corporate**

420. Subclause 126(4) requires that, with respect to an order sought to enforce a civil penalty under this Part, the penalty for a body corporate must not be more than 200 times the pecuniary penalty specified for the civil penalty provision. This subclause applies paragraph 82(5)(a) of the RPA Act as if “5 times” were omitted and “200 times” were substituted. At the time of introduction, this amounts to a maximum penalty of close to $10 million. This maximum penalty is proportionate, noting the policy objectives to combat serious criminal activity through the Schedule, and will ensure that large, multi-national communications providers that may be issued IPOs pursuant to this Schedule are sufficiently deterred from failing to comply with an order.

**Extra-territorial application**

421. Subclause 126(5) provides Part 4 of the RPA Act, as it applies in relation to a civil penalty provision in this Part, extends to acts, omissions, matters and things outside Australia.

**Part 9 - Reporting and record-keeping requirements**

**Division 1 - Introduction**

422. Clause 127 provides a simplified outline of Part 9, as introduced by the Bill. It briefly describes the framework for recordkeeping and reporting for agencies that can seek an IPO under Parts 2, 3, and 4, and for the Australian Designated Authority.
Division 2 - Reporting requirements

Annual reports by relevant agencies about International Production Orders

423. Clause 128 lists the matters which relevant agencies must report to the Minister with respect to their use of IPOs issued under Parts 2 and 3 of the Bill.

424. The chief officer of a relevant agency must provide the Minister the written report within three months after the end of each financial year. The reports go to the agency’s use of, and the effectiveness of the IPOs.

Reports to be made to the Attorney-General by the Director-General of Security

425. Clause 129 requires the Director-General of Security to provide a report to the Attorney-General on the usefulness of information obtained under an IPO for interception activities. These reports are to be provided within 3 months after the sooner of the order expiring, or the time when the order ceases to be in force because of revocation or cancellation.

426. This clause ensures that the Attorney-General has oversight of the use of IPOs relating to interception, for which he or she had consented to an application being made. This reporting measure is only required for IPOs relating to interception, recognising interception as an intrusive method of obtaining intelligence.

Annual reports by the Australian Designated Authority

427. Clause 130 requires the Australian Designated Authority to provide a report to the Minister with respect to IPOs under Parts 2 and 3 of the Bill, including, as relevant, their issue, cancellation, revocation and objection. The Australian Designated Authority will not report on matters relevant to IPOs issued under Part 3 of the Bill noting these matters will be included in the annual report of the Organisation.

428. The Australian Designated Authority must provide the Minister the written report within three months after the end of each financial year. Subclause 130(2) requires the Minister to cause a copy of the report to be given to the Attorney-General as soon as practicable after receiving the report. This is to provide the Attorney-General oversight of the functions of the Australian Designated Authority, noting the Secretary of the Attorney-General’s Department is the Australian Designated Authority.

Annual reports by the Minister

429. Clause 131 requires the Minister to prepare a written report that sets out, for each relevant agency, the information contained in a report made under clause 128, and the information contained in report made by the Australian Designated Authority under clause 130.

430. Subclauses 131(1) and (2) require the report to be prepared as soon as practicable after the end of each financial year, and to be tabled in each House of Parliament by the Minister within 15 sitting days of that House after the report is prepared.
431. So as not to prejudice investigations, subclause 131(3) prohibits the report from being made in a way that is likely to enable the identification of a person.

432. As per item 4 of the Bill, reporting requirements relevant to the Organisation’s use of Part 4 of the Bill are inserted into the existing annual reporting provision in the *Australian Security Intelligence Organisation Act 1979*. The existing annual reporting provision deals with deletions from the report that the Minister considers necessary for security, privacy or other specified reasons.

*Deferral of inclusion of information in Ministerial report*

433. Clause 132 sets out circumstances where the Minister must not include information that is considered to be control order information in the next Ministerial report. Clause 132 broadly aligns with reporting requirements that are applied to control order information in Australia’s current regime. It is intended to recognise that control orders have been sought and made only rarely, with the effect that it is uncommon for there to be more than a limited number of control orders in force at any given time. If the Minister were required to contemporaneously report publicly on 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 to a control order is or is not also subject to covert surveillance.

434. Subclause 132(1) sets out the scope of this clause applies to information included in a report to the Minister under clause 128 by the chief officer of a relevant agency; or under clause 130 by the Australian Designated Authority and information that, apart from this clause, is a required inclusion in the next Ministerial report.

*Exclusion of information—relevant agency*

435. Subclause 132(2) sets out that, in the case of a report by the chief officer of a relevant agency, the chief officer of the relevant agency is satisfied that the information is control order information, the chief officer must advise the Minister in writing not to include the information in the next Ministerial report.

436. Subclause 132(3) establishes that, if the Minister is satisfied, on the advice of the chief officer, that the information is control order information, the Minister must notify the chief officer in writing and not include the information in a Ministerial report until the Minister decides otherwise under subclause 132(5).

*Inclusion of information in subsequent report—relevant agency*

437. Subclause 132(4) sets out that when the information has not been included in a Ministerial report because of subclause 132(3), the chief officer must, before the Minister prepares the next Ministerial report, reconsider whether the information is control order information; and, if the chief officer is satisfied that the information is not control order information, advise the Minister in writing to include the information in the next Ministerial report.

438. Subclause 132(5) establishes that, if the Minister is satisfied, on the advice of the chief officer, that the information is not control order information, the Minister must notify the chief officer in writing; and include the information in the next Ministerial report.
Exclusion of information—Australian Designated Authority

439. Subclause 132(6) sets out that, in the case of a report by the Australian Designated Authority, the Australian Designated Authority is satisfied that the information is control order information, the Australian Designated Authority must advise the Minister in writing not to include the information in the next Ministerial report.

440. Subclause 132(7) establishes that if the Minister is satisfied, on the advice of the Australian Designated Authority, that the information is control order information, the Minister must notify the Australian Designated Authority in writing; and not include the information in any Ministerial report until the Minister decides otherwise under subclause (9).

Inclusion of information in subsequent report—Australian Designated Authority

441. Subclause 132(8) ensures that when information has not been included in a Ministerial report because of subclause 132(7), the Australian Designated Authority must, before the Minister prepares the next Ministerial report reconsider whether the information is control order information; and if the Australian Designated Authority is satisfied that the information is not control order information, advise the Minister in writing to include the information in the next Ministerial report.

442. Subclause 132(9) sets out that if the Minister is satisfied, on the advice of the Australian Designated Authority, that the information is not control order information, the Minister must notify the chief officer in writing; and include the information in the next Ministerial report.

Definitions

443. Subclause 132(10) defines control order information as information that, if made public, could reasonably be expected to enable a reasonable person to conclude that an IPO is likely to be, or is not likely to be, in force under Part 3 of this Schedule in relation to an inclusive list of services, stored communications, telecommunications data, or a particular person.

Division 3 - Record-keeping requirements

Keeping documents associated with International Production Orders—relevant agencies

444. Clause 133 requires the chief officer of a relevant agency to cause certain documents to be kept in the agency’s records. This requirement will assist the agency to fulfil its annual reporting requirements under Division 2 of this Part, and will facilitate effective oversight of the agency’s use of the IPO framework.

445. Subclause 133(2) requires the chief officer of the agency to cause a record kept under subclause 133(1) to be kept for 3 years, or when the Ombudsman gives a report to the Minister under clause 150 in relation to the record kept, whichever is sooner.

Other records to be kept—relevant agencies

446. Clause 134 requires the chief officer of a relevant agency to cause other relevant documents to be kept in the agency’s records. Subclause 134(2) gives the Minister the power
to prescribe, by legislative instrument, additional documents or material that must be caused to be kept on record by the chief officer of a relevant agency.

447. Subclause 134(3) requires the chief officer of the agency to cause a record kept under subclause 134(1) to be kept for 3 years, or when the Ombudsman gives a report to the Minister under clause 150 in relation to the record kept, whichever is sooner.

Keeping documents associated with International Production Orders—the Organisation

448. Clause 135 requires the Director-General of Security to cause certain documents to be kept in the Organisation’s records. This requirement will assist the Organisation to fulfil its annual reporting requirements, and will facilitate effective oversight of the Organisation’s use of the IPO framework by the IGIS.

449. Subclause 135(2) requires the Director-General of Security to cause a record kept under subclause (1) to be kept for 3 years.

Other records to be kept—the Organisation

450. Clause 136 requires the Director-General of Security to cause other relevant documents to be kept in the Organisation’s records. Subclause 136(2) requires the Director-General of Security to cause a record kept under subclause (1) to be kept for 3 years.

Keeping documents associated with International Production Orders—Australian Designated Authority

451. Clause 137 requires the Australian Designated Authority to cause certain documents to be kept in their records. This requirement will assist the Australian Designated Authority to fulfil its annual reporting requirements under Division 2 of this Part, and will facilitate effective oversight of the Australian Designated Authority’s role in the IPO framework.

452. Subclause 137(2) requires the Australian Designated Authority to cause a record kept under subclause (1) to be kept for 3 years.

Other records to be kept—Australian Designated Authority

453. Clause 138 requires the Australian Designated Authority to cause other relevant documents to be kept in the Australian Designated Authority’s records. Subclause 138(3) requires the Australian Designated Authority to cause a record kept under subclauses (1) and (2) to be kept for 3 years.

Division 4 - Register of International Production Orders

454. Clause 139 requires the Australian Designated Authority to cause a register to be kept of all IPOs issued under Schedule 1. The establishment of a register under this clause is to assist the Ombudsman to oversight agency use of the IPO framework.
Division 5 - Destruction of records

Destruction of records

455. Clause 140 requires that information obtained under an IPO issued under Parts 2, 3 or 4 of Schedule 1 relating to interception activities or stored communications, must be destroyed in circumstances where the information is in the agency or the Organisation’s possession, and the chief officer of the agency or the Director-General of Security is satisfied the records are not likely to be required for a purpose referred to in Part 11. This will ensure that records of sensitive, personal communications are not kept by agencies where no longer needed.

456. The destruction of telecommunications data obtained under an IPO is not required by this clause and is in line with current arrangements in the TIA Act. This view is supported by the Attorney-General’s Department in their response to recommendation 28 of the Parliamentary Joint Committee on Intelligence and Security’s Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. Among other things, the Attorney-General’s Department’s response found:

- Keeping telecommunications data for extended periods of time can be beneficial to law enforcement agencies in particular circumstances.
- A destruction requirement may have little privacy benefit and could create a further burden on the telecommunications industry.
- It will be administratively challenging to destroy copies of telecommunications data given its need to be stored on numerous information management systems.

Part 10 - Oversight by the Commonwealth Ombudsman

457. Clause 141 provides a simplified outline of Part 10 of Schedule 1, as introduced by the Bill. This outlines the Ombudsman’s ability to inspect records of a relevant agency and the Australian Designated Authority to determine compliance with the Schedule. The Ombudsman must table the findings of these inspections in an annual report to the Minister.

Inspection of relevant agency records by the Ombudsman

458. Subclause 142(1) is an enabling provision that provides that the Commonwealth Ombudsman may inspect records of a relevant agency to determine the extent of compliance with this Schedule by the agency and its officers. This enables the function of inspecting the relevant agency’s records in order to ascertain compliance with its obligations under the Schedule, and empowers the Ombudsman to do anything incidental or conducive to that function. The Ombudsman has the additional function of reporting to the Minister about the results of the inspections under this Part.

459. Subclause 142(2) outlines the powers of the Ombudsman for the purposes of an inspection under Subclause 142(1).

460. Subclause 142(3) requires that, before inspecting records of a relevant agency under this clause, the Ombudsman must give reasonable notice to the chief officer of the agency of when the inspection will occur. This is intended to allow the agency sufficient preparation.
time to ensure the necessary information is collated and available for the Ombudsman’s inspection.

461. Subclause 142(4) requires that the chief officer must ensure members of staff of the agency give the Ombudsman any assistance the Ombudsman reasonably requires to enable the Ombudsman to perform functions under this clause. This may include access to certain computer systems, locations within the agency’s premises, guidance personnel, and other assistance as required.

*Inspection of Australian Designated Authority records by the Ombudsman*

462. Clause 143 provides for the inspection of records of the Australian Designated Authority by the Ombudsman.

463. Subclause 143(1) provides that the Ombudsman may inspect records of the Australian Designated Authority to determine the extent of its compliance with this Schedule. This enables the function of inspecting the Australian Designated Authority’s records in order to ascertain compliance with its obligations under the Schedule, and empowers the Ombudsman to do anything incidental or conducive to that function. The Ombudsman has the additional function of reporting to the Minister about the results of the inspections under this Part.

464. Subclause 143(2) outlines the powers of the Ombudsman for the purposes of an inspection under Subclause 143(1).

465. Subclause 143(3) requires that, before inspecting records of the Australian Designated Authority under clause 143, the Ombudsman must give reasonable notice to the Australian Designated Authority of when the inspection will occur. This is intended to allow the Australian Designated Authority sufficient preparation time to ensure the necessary information is collated and available for the Ombudsman’s inspection.

466. Subclause 143(4) requires that the Australian Designated Authority must ensure members of staff of the Attorney-General’s Department give the Ombudsman any assistance the Ombudsman reasonably requires to enable the Ombudsman to perform functions under this clause. This may include access to certain computer systems, locations within the Department’s premises, guidance personnel, and other assistance as required.

467. Clause 144 enables the Commonwealth Ombudsman to obtain relevant information.

*Relevant agency*

468. Subclause 144(1) provides that, if the Ombudsman has reasonable grounds to believe that an officer of a particular relevant agency is able to give information relevant to an inspection under this Part of the agency’s records, the Ombudsman may:

- if the Ombudsman knows the officer’s identity, by written notice given to the officer, require the officer to do one or both of the following:
  - give the information to the Ombudsman, by writing signed by the officer, at a specified place and within a specified period;
  - attend before a specified inspecting officer to answer questions relevant to the inspection; or
• if the Ombudsman does not know the officer’s identity, require the chief officer of the agency, or a person nominated by the chief officer, to attend before a specified inspecting officer to answer questions relevant to the inspection.

**Australian Designated Authority**

469. Subclause 144(2) provides that, if the Ombudsman has reasonable grounds to believe that a member of staff of the Attorney-General’s Department is able to give information relevant to an inspection under this Part of the Australian Designated Authority’s records, the Ombudsman may:

• if the Ombudsman knows the member’s identity by written notice given to the member, require the member to do one or both of the following:
  o give the information to the Ombudsman, by writing signed by the member, at a specified place and within a specified period;
  o attend before a specified inspecting officer to answer questions relevant to the inspection; or

• if the Ombudsman does not know the member’s identity require the Australian Designated Authority, or a person nominated by the Australian Designated Authority, to attend before a specified inspecting officer to answer questions relevant to the inspection.

**Specification of place and period etc.**

470. Subclause 144(3) provides that a requirement to attend under subclauses 144(1)-(2) must specify a place for the attendance, and a period within which, or a time and day when, the attendance is to occur.

471. The place, and the period or the time and day, must be reasonable having regard to the circumstances in which the requirement is made. This is to take into account reasonable expectations regarding the requested officer’s or member’s availability.

**Offence**

472. Subclause 144(4) provides a person commits an offence if the person is subject to a requirement under subclauses 144(1) or (2); and the person omits to do an act; and the omission breaches the requirement. This includes failing to attend for the purposes of subclause 144(3), refusing to answer a question when directed without sufficient reason, or failing to provide a document when directed without sufficient reason.

473. The penalty for an offence against this subclause is imprisonment for 6 months, consistent with section 87 of the TIA Act.

474. Clause 145 provides that the Ombudsman is to be given information and access despite other laws.

475. Subclause 145(1) provides despite any other law, a person is not excused from giving information, answering a question, or giving access to a document, as and when required under this Part, on the ground that giving the information, answering the question, or giving
access to the document, as the case may be, would contravene a law; or be contrary to the public interest; or might tend to incriminate the person or make the person liable to a penalty.

476. Subclause 145(2) provides that the information or any information obtained as a result of giving the information is not admissible in evidence against the person. An exclusion to this is in a proceeding by way of a prosecution for an offence against clause 152 or an offence against Part 7.4 or 7.7 of the *Criminal Code*. Limiting the admissibility to only these offences is intended to encourage cooperation with the Ombudsman’s activities.

477. Subclause 145(3) provides nothing in clause 152 prevents an officer from giving information to an inspecting officer or giving access to a record of the relevant agency to an inspecting officer for the purposes of an inspection under this Part of the agency’s records. This is intended to allow for an officer to give as much detail as is necessary to the inspecting officer to complete their task.

478. Subclause 145(4) provides a relevant agency may make a record of information, provided for the purposes of giving the information to an inspecting officer. This record of information may be kept by both parties.

479. Subclause 145(5) provides nothing in clause 152 prevents a member from giving information to an inspecting officer or giving access to a record to an inspecting officer for the purposes of an inspection under this Part of the Australian Designated Authority’s records. This is intended to allow for a member to give as much detail as is necessary to the inspecting officer to complete their task.

480. Subclause 145(6) provides the Designated Authority may make a record of information, provided for the purposes of giving the information to an inspecting officer. This record of information may be kept by both parties.

481. Clause 146 provides for the application of the *Ombudsman Act 1976*.

482. Subclause 146(1) provides that section 11A of the *Ombudsman Act 1976*, referring to the powers of the Federal Court of Australia, does not apply in relation to the exercise or proposed exercise of a power, or the performance or the proposed performance of a function, of the Ombudsman.

483. Subclause 146(2) provides that a reference in section 19 of the *Ombudsman Act 1976*, referring to the provision of reports to Parliament, does not include a reference to anything that an inspecting officer has done or omitted to do under this Part.

484. Subclause 146(3) provides, subject to clause 145, subsections 35(2), (3), (4) and (8) of the *Ombudsman Act 1976* apply for the purposes of this Part, and lists the instances in which they would apply.

485. Clause 147 provides for the exchange of information between Ombudsman and State and Territory inspecting authorities. The effect of this provision is to enable the Ombudsman to communicate any accessed information to a State/Territory inspecting authority if it is relevant to the performance of the State/Territory inspecting authority’s function. The Ombudsman must be satisfied that giving the information is necessary to enable the inspecting authority to perform its functions in relation to the State/Territory inspecting authority.
486. Subclause 147(3) clarifies that the Ombudsman may receive, from an inspecting authority, information relevant to the performance of the Ombudsman’s functions under this Part.

487. Clause 148 provides for delegation by the Ombudsman.

488. Subclause 148(1) provides the Ombudsman may, by writing, delegate all or any of the Ombudsman’s powers under this Part other than a power to report to the Minister. This delegation can only be provided to an APS employee responsible to the Ombudsman or a person under the law of any state or territory whom is responsible to an oversight body with similar functions to the Ombudsman.

489. Subclause 148(2) requires that a delegate must, upon request of the person who is exercising the power of delegation, provide a written copy outlining their delegation powers for inspection by a person. The intent of this is to ensure that the delegated person outlines their authority to the affected person.

490. Clause 149 provides that the Ombudsman, an inspecting officer, or a person acting under an inspecting officer’s direction or authority, is not to be sued, or in relation to, an act or omission done in good faith in the performance or exercise, or the purported performance or exercise, of a function or power under this Part.

491. Clause 150 is a provision with respect to the reporting obligations of the Ombudsman.

492. Subclause 150(1) requires that the Ombudsman must report to the Minister, in writing, about the results of inspections of relevant agencies and the Australian Designated Authority during a financial year. Subclause 150(2) requires that the report must be given to the Minister as soon as practicable after the end of the financial year.

493. Subclause 150(3) requires that the Minister must cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives it. This timing is consistent with other reports provided by the Ombudsman.

494. Subclause 150(4) provides the Ombudsman may report to the Minister in writing at any time about the results of an inspection and must do so if so requested by the Minister.

495. Subclauses 150(5) and 150(6) provide that if, as a result of an inspection of the records of a relevant agency or the Australian Designated Authority, the Ombudsman is of the opinion that an officer of the agency, or a member of staff of the Attorney-General’s Department, has contravened a provision of this Schedule, the Ombudsman may include a report on the contravention in his or her report.

496. Subclause 150(7) requires that the Ombudsman must give a copy of relevant parts of a report produced under subclauses 150(1) or (4) to the chief officer of a relevant agency and the Australian Designated Authority, as relevant.

497. Subclause 150(8) requires that a report under clause 150 must not include information which, if made public, could reasonably be expected to endanger a person’s safety, prejudice an investigation or prosecution, or compromise any relevant agency’s operational activities or methodologies.
Part 11 - Disclosure of protected information

498. Clause 151 provides a simplified outline of Part 11 of Schedule 1, as introduced by the Bill.

Prohibition on use, recording, communication or publication of protected information or its admission in evidence

499. Clause 152 prohibits the use, recording, communication or publication of protected information, and its admission in evidence in any proceeding in Australia. A person commits an offence punishable by up to 2 years imprisonment if they use, record, communicate or publish protected information in a manner not permitted under Part 11. This clause is intended to protect the privacy of persons whose communications and information have been obtained pursuant to an IPO, and to control the disclosure of highly sensitive information pertaining to law enforcement and national security investigations that could prejudice investigations or compromise law enforcement and national security outcomes.

500. Protected information is defined in clause 2 to mean information in relation to, or obtained in accordance with, an IPO.

501. Clause 152 is intended to reflect the approach taken in Part 6, Division 1 of the Surveillance Devices Act 2004, and TIA Act, with respect to prohibitions on the use and disclosure of information obtained under those Acts.

General exceptions to prohibition

502. Clause 153(1) provides general exceptions to the prohibition in clause 152.

503. Subclause 153(1)(a) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of investigating a serious category 1 offence or serious category 2 offence. This is intended to include a Commonwealth, state or territory offence. Serious category 1 offence and serious category 2 offence are defined in clause 2. This exception also applies to the making of a report on the outcome of such an investigation.

504. Subclause 153(1)(b) allows for the use, recording, communication or publication of protected information for the purposes of making a decision whether or not to bring a prosecution for a serious category 1 offence or a serious category 2 offence. This is intended to include a Commonwealth, state or territory offence. This exception does not apply where subclause 153(1)(r) would apply.

505. Subclause 153(1)(c) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of a prosecution for a serious category 1 offence or a serious category 2 offence. This is intended to include a Commonwealth, state or territory offence. This exception does not apply where subclause 153(1)(r) would apply.

506. Subclause 153(1)(d) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of bail application proceedings in connection with a prosecution for a serious category 1 offence or a serious category 2 offence. This is intended to include a Commonwealth, state or territory offence.
Subclauses 153(1)(e) and (f) create similar exceptions in relation to proceedings to review a decision to refuse or grant a bail application referred to in subclause 153(1)(d).

507. Subclause 153(1)(g) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of investigating a contravention of the civil penalty provisions in the Schedule. The civil penalty provisions are set out in Part 8. This exception also applies to the making of a report on the outcome of such an investigation.

508. Subclause 153(1)(h) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of the performance of the functions, or the exercise of the powers, of the Organisation. This is intended to include communication of protected information to, and use of protected information by, the Organisation where the protected information relates or appears to relate to the functions and powers of the Organisation under the Australian Security Intelligence Organisation Act 1979. This exception is also intended to include the communication of protected information to, and use of protected information by, employees of the Organisation in the performance of their official functions and duties.

509. Subclause 153(1)(i) allows for the use, recording, communication, publication or admission in evidence of protected information for purposes in connection with Division 104 of the Criminal Code on control orders. This exception does not apply to control orders under state or territory laws.

510. Subclause 153(1)(j) allows for the use, recording, communication, publication or admission in evidence of protected information for purposes in connection with a preventative detention order law. This is intended to enable Commonwealth, state and territory agencies to use or disclose protected information in relation to their respective preventative detention order regimes, including in the following Acts:

- Criminal Code Act 1995 (Cth)
- 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

511. Subclause 153(1)(k) allows for the use, recording, communication, publication or admission in evidence of protected information for purposes in connection with Division 105A of the Criminal Code on continuing detention orders. This exception does not apply to any continuing detention orders under state or territory laws.
512. Subclause 153(1)(l) allows for the use, recording, communication, publication or admission in evidence of protected information for the purpose of an application for a civil penalty order relating to a contravention of a civil penalty provision under Part 8 of this Schedule.

513. Subclauses 153(1)(m) and (n) allow for the use, recording, communication and publication of protected information for the purposes of record keeping and reporting under the Schedule and reporting under subsection 94(1) of the Australian Security Intelligence Organisation Act 1979, insofar as such reporting includes statements covered by subsection 94(2BBA) of that Act.

514. Subclauses 153(1)(o), (p) and (q) allow for the use, recording, communication and publication of protected information for the purposes of an inspection by the Ombudsman under clause 142 or 143, the performance of functions and exercise of powers by the IGIS under the Inspector-General of Intelligence and Security Act 1986 and by an Ombudsman official under the Ombudsman Act 1976. This is intended to include communication of protected information to, and use of protected information by, the Ombudsman and IGIS.

515. Subclause 153(1)(r) allows for the use, recording, communication, publication or admission in evidence of protected information for purposes of investigations under the Privacy Act 1988 or any other Commonwealth law concerning the privacy of personal information. This subclause also clarifies that disclosure of protected information is also permitted for the purpose of any subsequent investigation or prosecution of a serious category 1 offence or serious category 2 offences arising directly from the first-mentioned investigation, despite the fact that such a use, recording, communication, publication or admission in evidence of protected information would otherwise not be permitted under this subclause.

516. Subclause 153(s) allows for the use, recording, communication, publication and admission as evidence of protected information for the purposes of the administration or execution of this Schedule. This is designed to permit disclosure for the purposes of any acts done in administering or carrying out any part of this Schedule.

517. Subclause 153(t) allows for the use, recording, communication, publication and admission as evidence of protected information for the purposes of legal proceedings arising out of or related to this Schedule. This is intended to include, for example, any proceedings relating to a breach of the prohibition in clause 152. This exception also applies to any report of such proceedings.

518. Subclause 153(1)(u) allows for the use, recording, communication, publication and admission in evidence of protected information for the purposes of taking of evidence under section 43 of the Extradition Act 1988, in so far as the proceeding relates to a serious category 1 offence.

519. Subclause 153(1)(v) allows for the communication of protected information to, and the use of protected information by, a foreign country in accordance with section 13 of the Mutual Assistance in Criminal Matters Act 1987, provided that such communication or use is in relation to an offence against the law of that foreign country that is punishable by a term of imprisonment of three years or more, or life. This will ensure consistency of threshold with a serious category 1 offence.
Subclauses 153(1)(w) and 153(x) allows for the communication of protected information to, and the use of information by, the International Crime Court in connection with proceedings under Division 5 of Part 4, and Part 5, of the International Criminal Court Act 2002.

Subclause 153(1)(y) allows for the communication of protected information to, and the use of information by, the International War Crimes Tribunal in connection with proceedings under Division 1 of Part 4 of the International War Crimes Tribunals Act 1995.

Subclause 153(1)(z) allows for the use, recording, communication and publication of protected information for purposes in connection with a designated international agreement. This is intended to include the communication of protected information to, and use of information by governments in order to give effect to a designated international agreement, or for purposes required by or contemplated by the designated international agreement. For example, this exception would cover communication of protected information between the Australian Government and a foreign government with which Australia has a designated international agreement during discussions regarding the implementation of that agreement.

Subclause 153(2) clarifies that, for the purposes of the exceptions in subclause 153(1), the Schedule is taken to include the Regulatory Powers (Standard Provisions) Act 2014, so far as Regulatory Powers (Standard Provisions) Act 2014 relates to the Schedule.

Disclosure to the Public Interest Monitor (PIM) of Victoria or Queensland

Subclauses 153(3) and (4) permit the notification, or giving of information, to the PIM of Victoria or Queensland. This will assist in the ability of the PIM to make submissions to the eligible Judge or nominated AAT member when a Victorian or Queensland interception agency or control order agency makes an application to those authorities.

International assistance

Subclauses 153(5), (6) and (7) ensure that protected information can be provided to foreign countries and international bodies such as the International Criminal Court and International War Crimes Tribunal. This accords with current practice in terms of information that agencies have obtained under the domestic regimes within the TIA Act. The Attorney-General has the discretion to authorise disclosure of protected information under the Mutual Assistance in Criminal Matters Act 1987, the International Criminal Court Act 2002, and the International War Crimes Tribunals Act 1995.

Disclosure to Ministers

Clause 154 allows protected information to be communicated to the Minister for the purposes of the performance of the Minister’s functions, or the exercise of the Minister’s powers. This is intended to include the communication of protected information to the Minister that relates or appears to relate to any of the Minister’s functions or exercise of any of the Minister’s powers across all subject matters that the Minister is responsible for.

Clause 155 allows protected information to be communicated to the Attorney-General for the purposes of the performance of the Attorney-General’s functions, or the exercise of the Attorney-General’s powers. This is intended to include the communication of protected information to the Attorney-General that relates or appears to relate to any of the Attorney-General’s functions or exercise of any of the Attorney-General’s powers across any subject
matters that the Attorney-General is responsible for. Disclosures to the Attorney-General are permitted under this clause in recognition of the Australian Designated Authority being the Secretary of the Attorney-General’s Department, and the Attorney-General’s functions and responsibilities as the First Law Officer of the Commonwealth.

Disclosure of statistical information by designated communications providers

528. Clause 156 allows designated communications providers to disclose the total number of IPOs that they have been given by the Australian Designated Authority during a period of at least six months. A note is inserted into this clause to clarify that the clause only permits the disclosure of aggregate statistical information that cannot be broken down by agency that obtained the order or in any other way, for example by the type of order or type of data requested. This clause is intended to balance the interests of designated communications providers in reporting on their activities to shareholders and publicly for transparency reasons, with the need to limit public disclosure of highly sensitive information pertaining to law enforcement and national security investigations that could prejudice investigations or otherwise compromise law enforcement and national security outcomes.

Specific exceptions relating to International Production Orders for interception

529. Clause 157(1) provides additional exceptions to the prohibition in clause 152 in relation to the use, recording, communication, publication and admission in evidence of protected information that was obtained under, or relates to, an IPO relating to interception. These exceptions include use and disclosure for purposes in connection with a range of Commonwealth, state and territory proceedings and eligible purposes of a range of Commonwealth, state and territory agencies. Eligible purpose is defined in subclause 157(2).

530. These exceptions are intended to be consistent with the exceptions in sections 5 and 5B of the TIA Act.

Specific exceptions relating to International Production Orders for stored communications

531. Clause 158 provides additional exceptions to the prohibition in clause 152 in relation to the use, recording, communication, publication and admission in evidence of protected information that was obtained under, or relates to, an IPO relating to stored communications. These exceptions include use and disclosure for purposes in connection with a range of Commonwealth, state and territory proceedings.

532. These exceptions are intended to be consistent with the exceptions in section 5 insofar as they apply to Chapter 3 of the TIA Act, and sections 134–146 of the TIA Act.

Specific exceptions relating to telecommunications data

533. Clause 159 provides additional exceptions to the prohibition in clause 152 in relation to the use, recording, communication, publication and admission in evidence of protected information that consists of telecommunications data obtained under an IPO or which relates to such an IPO.

534. Subclause 159(1) allows use and disclosure of protected information covered by subclauses 159(1)(a) and (b) for purposes in connection with enforcement of a criminal law or law imposing a pecuniary penalty or the protection of the public revenue. This is intended to include a law or the public revenue of the Commonwealth, a state or territory.
535. Subclause 159(2) allows protected information covered by subclause (1)(a) and (b) to be used or disclosed for the purpose of finding a missing person, or disclosed to the person who notified the AFP or state police force in certain circumstances set out in subclause 159(2)(b).

536. These exceptions are intended to be consistent with the exceptions in sections 181A–182B of the TIA Act.

**Part 12 - Evidentiary certificates**

537. Clause 160 provides a simplified outline of Part 12 of Schedule 1, as introduced by the Bill.

**Evidentiary certificates – compliance with International Production Orders**

538. Subclause 161(1) and (2) provide that a provider or a manager of the designated communications provider may issue a signed written certificate setting out facts detailing acts or things done by the provider in order to comply with the IPO. A manager may include any individual who is involved in the management of the provider and is able to authorise evidentiary certificates for that particular designated communications provider.

539. Subclause 161(3) permits a certificate issued under subclause 161(1) or (2) to be received in evidence in a proceeding in Australia without further proof, and the certificate is to be **conclusive** evidence of the matters stated in the document in those proceedings.

540. Taking the designated communications provider’s evidentiary certificate as **conclusive** evidence of the matters stated in the document ensures that employees of the provider are not required to testify in each proceeding where evidence obtained under an IPO is adduced. Current practices within the TIA Act for domestic interception, access to stored communications and telecommunications data allow for evidentiary certificates. The use of evidentiary certificates for IPOs is of significant utility as requiring the appearance of employees of foreign designated communications providers to court proceedings held in Australia will be complex and, at times, impractical. This also recognises the novel fact that whilst it will be easier to obtain information by virtue of the new order framework, Australian prosecutorial and law enforcement bodies will not be able to compel foreign provider employees to attend court to give evidence.

**Voluntary provision of associated information by designated communications providers**

541. Clause 162 allows designated communications providers to issue a signed written certificate in relation to information voluntarily provided in connection with an IPO.

542. Subclause 162(7) permits a certificate issued under clause 162 to be received in evidence in a proceeding in Australia without further proof, and the certificate is to be **prima facie** evidence of the matters stated in the document in those proceedings, so long as the information obtained in accordance with the IPO is admissible in those proceedings.

543. This provision seeks to provide agencies the ability to adduce as evidence in a proceeding, information or material voluntarily provided by a designated communications provider in addition to the material or information provided to comply with an IPO. This provision ensures where a designated communications provider wishes to provide additional information voluntarily in response to an IPO, the voluntarily provided information is also
able to be adduced in court proceedings in the event it is admissible. This evidentiary certificate ensures that where a designated communications provider discloses information voluntarily, or explanatory material to assist in the understanding of information obtained under an IPO, there is a mechanism to allow for the evidence to be received as prima facie evidence in a proceeding. The voluntary disclosure or the explanatory material must be in connection with the IPO.

544. The reference to in connection under clause 162 is intended to operate flexibly. For example, if the designated communications provider receives an order and has identified other services associated with the person of interest identified in the order, the designated communications provider may disclose subscriber information or other non-content data to the law enforcement agency.

Evidentiary certificates - Interception

545. Clause 163 provides that a certifying officer of an interception agency, control order IPO agency, and the Organisation may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to the receipt by the agency of intercepted material or information pursuant to Parts 2, 3 and 4 of item 43 of the Bill. This clause also provides for the receipt of telecommunications data disclosed in accordance with an IPO seeking interception activities.

546. Certificates issued under this clause are to be received in evidence in a proceeding in Australia without further proof, and are prima facie evidence of the matters stated in the document. This ensures that employees or officers of the agency are not required to testify in each proceeding that the material or information was lawfully obtained.

Evidentiary certificates -Stored communications

547. Clause 164 provides that a certifying officer of a criminal law-enforcement agency, control order IPO agency, and the Organisation may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to the receipt by the agency of stored communications pursuant to Parts 2, 3 and 4 of item 43 of the Bill. This clause also provides for the receipt of telecommunications data disclosed in accordance with an IPO seeking stored communications.

548. Certificates issued under this clause are to be received in evidence in a proceeding in Australia without further proof, and are prima facie evidence of the matters stated in the document. This ensures that employees or officers of the agency are not required to testify in each proceeding that the material or information was lawfully obtained.

Evidentiary certificates - Telecommunications data

549. Clause 165 provides that a certifying officer of enforcement agency, control order IPO agency, and the Organisation may issue a written certificate signed by the officer setting out such facts as the officer considers relevant with respect to the receipt by the agency of stored communications pursuant to Parts 2, 3 and 4 of item 43 of the Bill.

550. Certificates issued under this clause are to be received in evidence in a proceeding in Australia without further proof, and are prima facie evidence of the matters stated in the
document. This ensures that employees or officers of the agency are not required to testify in each proceeding that the material or information was lawfully obtained.

_Evidentiary certificates - Australian Designated Authority_

551. Subclause 166(1) provides for the Australian Designated Authority to issue a signed written certificate relating to the Australian Designated Authority giving an IPO, or giving an instrument of revocation, or giving an instrument of cancellation to a designated communications provider.

552. Subclauses 166(2)-(4) provides for the Australian Designated Authority to issue a signed written certificate relating to the Australian Designated Authority receiving material or information obtained under Parts 2, 3 and 4 of item 43 of the Bill from a designated communications provider, or things done by the Australian Designated Authority for ensuring the material or information was passed to the relevant agency which requested the information.

553. Certificates issued under this clause are to be received in evidence in a proceeding in Australia without further proof, and are _prima facie_ evidence of the matters stated in the document. This ensures that employees or officers of the Australian Designated Authority are not required to testify in each proceeding that the material or information was lawfully dealt with.

**Part 13 - Incoming orders and requests**

554. Part 13 of the Bill provides for exemptions from prohibitions on the interception and disclosure of information for acts done in compliance with an incoming order or request, or the issue of an order or making of a request, or information obtained in accordance with an order or request, issued by a competent authority of a foreign country with which Australia has a designated international agreement.

555. Clause 167 provides a simplified outline of Part 13 of Schedule 1, as introduced by the Bill.

556. Clause 168 provides details of the relevant exemptions, namely from:

- Subsections 7(1) and 108(1) of the TIA Act, which relate to the prohibition on interception of telecommunications and access to stored communications (respectively);

- Subsections 63(1) and 133(1) of the TIA Act, which relate to the prohibition on dealing with intercepted information and interception warrant information, and accessed information (respectively); and

- Sections 276, 277 and 278 of the _Telecommunications Act 1997_, which deal with the prohibition on, and offences relating to, the disclosure or use of certain information by current or former eligible persons, eligible number-database persons or emergency call persons (respectively).

557. Notes in the Part indicate that in a prosecution for an offence against the blocking provisions in the TIA Act, and the _Telecommunications Act 1997_, the defendant bears the evidential burden in accordance with section 13.3(3) of the _Criminal Code Act 1995_. This
means the defendant will bear the burden of adducing evidence that suggests a reasonable possibility that the accessing and disclosure of communications and information was for a purpose that is authorised by the Bill. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt.\textsuperscript{3}

558. This burden is placed on the defendant in these circumstances as the person acting in accordance with an order or request has the knowledge to address the matter, and it would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter. This position is supported by the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers.\textsuperscript{4}

559. Clause 169 relates to the interaction between provisions in the Bill and relevant provisions in the Privacy Act 1988, and in particular in relation to the disclosure of personal information in compliance with an order or request issued by a competent authority of a foreign country with a designated international agreement with Australia. It provides, in these circumstances, the disclosure of information is taken to be authorised by the TIA Act. This will ensure that Australian providers will not be in breach of the Privacy Act 1988 if they disclose information in response to an order or request issued or made by a foreign country where there is a relevant designated international agreement. In practice, it is expected that consideration of protections and safeguards related to privacy will also be a consideration when developing international agreements.

560. The phrasing of orders and requests ensures that Australian providers can lawfully respond to orders and requests for information permitted to be disclosed under a designated international agreement. For example, a request may be a lawful request for the disclosure of subscriber information, whilst an order may be a court order requiring the disclosure of content data.

**Part 14 - Miscellaneous**

561. Clause 170 provides a simplified outline of Part 14 of Schedule 1, as introduced by the Bill, including the electronic service of documents; certified copies of IPOs; and delegations.

*Electronic service of documents*

562. Clause 171 provides for the electronic service of particular documents between the Australian Designated Authority, designated communications providers, agencies, and the Organisation. However, this can only be done where the Australian Designated Authority or person has nominated an electronic address for service. The order, copy or instrument is taken to have been given to the person if sent to that nominated electronic address for service.

563. The service of documents to an electronic address is now a routine method for delivering documents. Documents submitted electronically can be sent and received faster than traditional postal methods, reducing turn-around times. The provision for electronic service of documents is consistent with the overall objectives of the Schedule to provide data effectively and efficiently across borders. A requirement that that the recipient must have nominated an electronic address for service will ensure that service is properly effected on the intended recipient.

\textsuperscript{3} Criminal Code Act 1995 (Cth) section 13.1.

\textsuperscript{4}[4.3.2].
International Production Order issued in response to a telephone application

564. Clause 172 sets out the action required by an applicant after an IPO is issued on a telephone application. This clause applies if an IPO is issued in response to a telephone application made on behalf of a relevant agency or the Organisation.

Required action

565. Subclause 172(2) provides that within one day of the IPO being issued, the applicant must cause each person who gave information to the issuing person for the application, to swear or affirm an affidavit setting out the information given, and give the affidavit or affidavits to the issuing person. If the applicant was authorised to make the application by telephone as a result of an authorisation under the relevant provisions, the applicant must also give the issuing person a copy of the authorisation.

566. This clause is designed to assign an appropriate level of accountability to an applicant for an IPO made by way of telephone application. While urgent circumstances may necessitate the application to be made by telephone, it is appropriate that within a period of one day, the applicant be required to provide the information given by way of affidavit.

Cancellation if required action not taken

567. Subclause 172(3) provides that the issuing person may cancel the order if satisfied that subclause 172(2) has not been complied with. Subclause 172(4) provides the cancellation must be set out in a written instrument.

568. The ability for the issuing person to be able to cancel the order on non-compliance with subclause 172(2) is an appropriate measure. While the flexibility of a telephone application is afforded for circumstances of urgency, it is necessary for transparency and accountability that the grounds for the application be provided in writing shortly after the order has been issued by such means.

569. Under subclause 172(5), if the IPO is so cancelled by the issuing person, the issuing person must give the instrument of cancellation to the Australian Designated Authority as soon as practicable after the order is cancelled. If the telephone application was made on behalf of a relevant agency, the Australian Designated Authority must inform the chief officer of the relevant agency of the cancellation as soon as practicable after the instrument of cancellation is given to the Australian Designated Authority. If the telephone application was made on behalf of the Organisation, the Australian Designated Authority must inform the Organisation of the cancellation as soon as practicable after the instrument of cancellation is given to the Australian Designated Authority.

570. Subclause 172(6) provides that if the Australian Designated Authority has already given the subsequently-cancelled IPO to the relevant designated communications provider, the Australian Designated Authority must give the instrument of cancellation to the designated communications provider as soon as practicable after that instrument is given to the Australian Designated Authority. This will ensure that the relevant designated communications provider is informed of the cancellation as soon as practicable, and will not invest time, resources, or further time or resources, towards compliance with the order.
571. Subclause 172(7) provides that if the instrument of cancellation is required to be given to the designated communications provider, the cancellation takes effect when the instrument is given. In all other cases, the cancellation takes effect when the cancellation is made.

572. Subclause 172(8) provides that if an IPO is cancelled under clause 172, and the Australian Designated Authority has not made a decision about giving the order under clause 111 or 112, that decision ceases to be available once the cancellation takes effect.

*Duty of nominated AAT Security Division member*

573. Clause 173 provides that a nominated AAT Security Division member has a duty to ensure, so far as possible, that in or in connection with actions under this Schedule, information is not communicated or made available to a person contrary to the requirements of security. This is consistent with the duty of the Tribunal in section 39B(11) of the AAT Act.

*Certified copies of International Production Orders*

574. Clauses 174 to 178 ensure that a document certified in writing by a relevant certifying officer or certifying person to be a true copy of an IPO, is to be received in evidence in mentioned proceedings as if it were the original IPO.

*Delegation by the Australian Designated Authority*

575. Subclause 179(1) permits the Australian Designated Authority to delegate by writing any or all of the Australian Designated Authority’s functions or powers under this Schedule to an SES/EL2/EL1 employee (including those acting in those positions) in the Attorney General’s Department. For clarity, a note is included that references section 2B of the *Acts Interpretation Act 1901*.

576. The ability to delegate, to an appropriately senior employee such as an executive or senior executive level employee, the functions or the powers of the Australian Designated Authority is important to streamline the day-to-day operations of the Australian Designated Authority, and is consistent with the approach taken in international crime cooperation more broadly.

577. Subclause 179(2) requires that a delegate must comply with any directions of the Australian Designated Authority when performing functions, or exercising powers under a delegation under subclause 179(1).

*Minor defects in connection with International Production Order*

578. Clause 180 provides that where information is purportedly obtained in accordance with an IPO, and there is a defect or irregularity in relation to the IPO, the information is taken to have been obtained in accordance with the IPO. It must be the case that apart from that defect or irregularity, the information would have been obtained in accordance with that IPO.

579. A defect or irregularity in relation to an IPO means one that is not a substantial defect or irregularity, and is in connection with the issue of a document purporting to be the IPO, or in connection with compliance with the IPO, or in connection with purported compliance
with a document purporting to be the IPO. The intention is to minimise evidence being excluded solely on the basis of a defect or irregularity.

Protection of persons - control order declared to be void

580. Subclause 181(1) provides a safeguard to protect from criminal proceedings a person acting in good faith in purported compliance with an IPO issued on the basis of an interim control order, where a court subsequently declares the interim control order on which the IPO was issued, to be void.

581. Subclause 181(2) provides subclause (1) does not apply if, at that time, the person knew, or ought reasonably to have known, of the declaration.

Specification of international agreements

582. Clause 182 provides for the specification of international agreements. It establishes that where there is an agreement between Australia and one or more foreign countries and the name of the agreement is specified in one of the items listed under subclause 182(b)(i)-(iv), a reference in the regulations, application, order or other instrument (as the case may be) to the agreement is a reference to the agreement as amended and in force for Australia from time to time.

583. Clause 182 is included for the avoidance of any doubt as to whether a reference to an agreement made under the Bill is both current and intended, as the specified agreement will be included under the Bill’s regulations. This will make the agreement material that can be looked to in ascertaining any policy intention or meaning underlying the Bill, and this will further ensure that both section 14 of the Legislation Act 2003 and section 46AA of the Acts Interpretation Act 1901 do not place limits on the way an agreement can be incorporated into legislation by reference.

Operation of the Mutual Assistance in Criminal Matters Act 1987 not limited

584. Clause 183 ensures that the Schedule is not taken to limit the operation of the Mutual Assistance in Criminal Matters Act 1987. The framework set up in the Schedule is separate and does not derogate from the mutual legal assistance processes.

Other functions or powers not limited

585. Clause 184 provides the Schedule is not intended to limit the powers or functions of relevant agencies, the Organisation, or any other body or person, in requesting or obtaining assistance or information from a designated communications provider or any other body or person. A body or person may, outside the IPO regime, request or obtain, or continue to request or obtain, information or assistance via any alternate means. The request for or obtaining of assistance or information does not need to be in response to the application of powers by that body or person, and may include voluntary disclosures or assistance.
Part 2 - Application and Transitional Provisions

Item 44 Application - declaration of eligible Judges

586. This item provides the amendment of subsection 6D(3) of the TIA Act made by this Schedule (see items 14 and 15 above) applies in relation to a declaration made after the commencement of this item.

Part 3 - Amendment contingent on the commencement of the Federal Circuit and Family Court of Australia

Telecommunications (Interception and Access) Act 1979

Item 45 Subclause 126(3) of Schedule 1

587. Item 45 is a contingency amendment relating to the relationship between clause 126 of Schedule 1, as introduced by the Bill, and the Federal Circuit and Family Court of Australia (Consequential Amendments and Transitional Provisions) Bill 2019. This item provides, on commencement of the Federal Circuit and Family Court of Australia Act 2020, the reference in subclause 126(3) to the Federal Circuit Court of Australia is to be omitted and substituted with a reference to the Federal Circuit and Family Court of Australia.

588. Subclause 126(3) of Schedule 1, as introduced by the Bill, relates to the relevant courts in relation to a civil penalty provision in Part 6 of Schedule 1, for the purposes of Part 4 of the Regulatory Powers (Standard Provisions) Act 2014.

Part 4 - Minor amendment

Surveillance Devices Act 2004

Item 46 Subsection 42(6)

589. Item 46 amends subsection 42(6) of the Surveillance Devices Act 2004 to provide that, in circumstances where evidence in writing is required that certain surveillance has been agreed to by an appropriate consenting foreign official, that evidence must be given by the chief officer of the law enforcement agency which applied for a warrant authorising the surveillance to the Minister for Home Affairs, and not to the Attorney-General. This is a minor amendment correcting an earlier drafting error.

Telecommunications (Interception and Access) Act 1979

Item 47 Subsection 6DA(1)

590. This item removes the ability for nominated AAT members to issue warrants under Part 3-3 of the TIA Act.

Item 48 Subsection 6DA(4)

591. This item removes reference to ‘3-3’, as it becomes redundant from the removal in item 47.
Item 49    Transitional - nomination of AAT member

592.  Subitems (1) and (2) clarify that the amendments made under items 47 and 48 apply to nominations under section 6DA in force immediately before the commencement of the Bill. This also ensures endurance of existing nominations whilst removing redundant references. This does not change what current nominated AAT members can authorise, as the reference to Part 3-3 was redundant and did not permit AAT members to authorise stored communications warrants. Only issuing authorities are permitted to do so.