



Australian Government  

---

Department of Home Affairs

# **Preliminary submission to the Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020**

Parliamentary Joint Committee on Intelligence and Security

# Table of Contents

<b>Introduction</b>	<b>3</b>
<b>The policy challenges of communications technology and serious crime</b>	<b>3</b>
Changing communications landscape and criminal use of communications technology	3
International crime cooperation	3
Conflict of laws	4
Paradigm shift of cross-border access to electronic data	4
The Telecommunications Legislation Amendment (International Production Orders) Bill 2020	5
The purpose of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020	5
Outgoing order process – International production orders	5
Oversight and accountability	7
The requirement for an Australian Designated Authority	8
Enforcement and compliance	8
Evidentiary requirements and admissibility	9
Incoming order process – foreign orders and requests	9
Minor amendments	10
Consultation	10
<b>Appendix A – Comparison table: Authorising authorities under the international production order framework and the domestic TIA Act framework</b>	<b>11</b>
<b>Appendix B – Key criteria for authorising an international production order</b>	<b>12</b>
<b>Appendix C - Types of evidentiary certificates for international production orders</b>	<b>13</b>

## Introduction

1. To assist the Committee early in the Parliamentary Committee process, this preliminary submission by the Department of Home Affairs provides an overview of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ('the Bill'), and the policy challenges behind the need for this legislative reform. The Department of Home Affairs intends to provide a supplementary submission including case examples/case studies.

## The policy challenges of communications technology and serious crime

### Changing communications landscape and criminal use of communications technology

2. In 2018, the Australian Bureau of Statistics Internet Activity Survey reported that there were 14.7 million internet subscribers in Australia. There were also approximately 27 million mobile handset subscribers. Australia is clearly a networked society.
3. Where this communications technology generates electronic data relevant to the investigation and prosecution of serious crime, governments have used domestic electronic surveillance laws to require communications service providers (CSPs) (such as carriers and carriage service providers) within their jurisdiction to disclose such data. Over many decades, the communications technology landscape has shifted significantly, reflecting the changing ways in which the globe communicates. Home telephony is now largely replaced by mobile and internet connections, with the use of over-the-top applications, messaging and voice-over-IP (Internet Protocol address).
4. Many of these applications and services are provided or offered by foreign CSPs with global operations. But smaller bespoke communications services offered on the internet can also be globally accessible. In many cases, the internet or messaging applications are used to facilitate or obfuscate criminal conduct and do not require the person to have any technical capabilities or knowledge.

### International crime cooperation

5. It follows that electronic data is often kept offshore. For example, the United States has a significant proportion of the world's CSPs and is a major data-controller within the modern world. Communications data also regularly moves across geographical borders, through servers and other infrastructure located around the globe, meaning the exact location of data and relevant jurisdiction may be difficult for law enforcement and national security agencies to determine.
6. International crime cooperation mechanisms (such as mutual legal assistance) remain the principal means to obtain evidence, including electronic data, from foreign jurisdictions for use in criminal investigations and prosecutions. However, the digital world and the rapid increase in digital evidence for all types of criminal offences – not just cyber offences – is fundamentally undermining international crime cooperation. The traditional mechanism of mutual legal assistance has proven to be a slow and cumbersome way of working, not responding sufficiently to this fundamental shift in the offshore storage of Australians' data.
7. The pressure placed on existing mechanisms is significant, and is exacerbated by the increasingly global operations of CSPs who are subject to the laws of multiple jurisdictions, or the location of the relevant data being undetermined because of the nature of international data flows. On average, it takes 10-12 months before an Australian agency receives electronic data for a criminal matter through this process (some matters have taken up to 18 months). This delay can mean that while investigations cannot be progressed, criminals continue to offend and victimise, and take advantage of the complexities of

electronic evidence gathering across jurisdictions. For example, if electronic evidence cannot be obtained in accordance with court timeframes, this can result in charges being withdrawn, less serious charges being laid or a weaker case going before the court which does not show the full picture of criminality, and may ultimately lead to lower sentences being imposed, if at all.

8. This is not an issue unique to Australia; the challenges of government-to-government international crime cooperation continue to be acknowledged internationally. As an example, the Cybercrime Convention Committee (T-CY) for the Council of Europe Budapest Convention on Cybercrime reported in 2015 that inefficiencies in these processes lead to abandoned requests and investigations.<sup>1</sup> Building on this work, a further special T-CY working group was established (the T-CY Cloud Evidence Group) that reported in 2016<sup>2</sup> that while these processes are inefficient in general, with respect to electronic data, the use of mutual legal assistance is not always a realistic solution to access evidence in the context of remotely stored data (cloud storage).

## Conflict of laws

9. Circumstances where foreign CSPs hold electronic data relevant to offshore criminal matters often involve a complex web of legal compliance and regulation. It also significantly frustrates agencies' access to electronic data to combat crime, putting the Australian community at risk.
10. CSPs with global operations may be subject to multiple countries' laws restricting the disclosure of certain electronic data. For example, foreign jurisdictions may heavily restrict the disclosure of the content of communications, or prevent the disclosure of that information in its entirety without a mutual legal assistance request. Where foreign CSPs store data in third party foreign jurisdictions, they may be subject to laws of the country in which they operate, the laws of the country where the data is stored, and the laws of the country with jurisdiction over the criminal matter.

## Paradigm shift of cross-border access to electronic data

11. In 2018, the United States introduced the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). This has been recognised as a significant shift towards a new paradigm, which supports efficient and effective cross-border access to the electronic data needed to combat serious crime, while safeguarding privacy and human rights.
12. The CLOUD Act has two pillars. Firstly, it authorises the United States to enter into executive agreements with other countries that meet certain criteria, such as the rule of law and privacy protections, and removal of any 'blocking statutes' between jurisdictions. 'Blocking statutes' are understood to be the relevant prohibitions in each countries' domestic laws that prevent either access to, or disclosure of, electronic data. Secondly, the CLOUD Act clarifies at law that a CSP under United States jurisdiction is compelled to produce data that it controls or possesses in the operation of its service in response to relevant legal process in the United States. The latter was not a new principle and clarified the United States domestic legal position in response to the Microsoft case<sup>3</sup>.
13. The first pillar permits a qualifying foreign government with whom the United States has an agreement to go directly to US-based CSPs with legal process, rather than needing to go through the United States government (and vice versa). Noting that the United States is the largest data controller in terms of communications technologies, services and platforms, entering such an agreement with the United States would have significant benefits to Australian law enforcement and national security efforts.

---

<sup>1</sup> Cybercrime Convention Committee (T-CY) '*Criminal justice access to data in the cloud: challenges*'. Australia is a signatory to the Budapest Convention on Cybercrime since 2012.

<sup>2</sup> T-CY Cloud Evidence Group '*Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*'.

<sup>3</sup> *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016).

14. Australia is likely to be the next qualifying foreign government to enter into an agreement with the United States (after the United Kingdom, who finalised an agreement with the United States in October 2019). On 7 October 2019, Australia and the United States announced the commencement of formal negotiations for a bilateral agreement pursuant to the CLOUD Act.

## **The Telecommunications Legislation Amendment (International Production Orders) Bill 2020**

15. The Bill sets out a framework to enable Australia to give effect to such bilateral or multilateral agreements. It stands up a new international production order (IPO) framework that allows Australian law enforcement and national security agencies to, amongst other things, issue extraterritorial orders for electronic data on foreign designated communications providers (DCPs) where there is an agreement in place. The IPO framework will complement other international crime cooperation mechanisms and is not intended to restrict other means of obtaining electronic data.

16. The Bill also removes the 'blocking statutes' for Australian providers to respond to foreign orders or requests from countries with whom Australia has an agreement.

## **The purpose of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020**

17. The Bill creates a new schedule (Schedule 1) to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to enable law enforcement and national security agencies to access electronic data in accordance with bilateral or multilateral agreements with foreign countries, by:

- a. creating a framework for Commonwealth, state and territory agencies to obtain independently-authorized IPOs for data from designated communications providers in foreign countries (outgoing orders); and
- b. permitting Australian carriers, carriage service providers and other relevant industry to disclose communications data in response to incoming orders or requests from a foreign country (incoming orders).

18. In all cases, there must be a "designated international agreement" in place to facilitate both the outgoing and incoming order processes. This ensures that the IPO framework is only used in circumstances where the Australian government has entered into an agreement with trusted partners.

## **Outgoing order process – International production orders**

### ***Shaping the international production orders - domestic legislation and international cross-border access to data agreements***

19. The IPO Bill sets up a broad framework, which is designed to facilitate a range of future bilateral and multilateral designated international agreements for cross-border access to data, recognising they may each have a range of requirements and restrictions. Each individually negotiated agreement will guide the operation of the framework via its specific provisions. For example, the 'CLOUD Act' agreement signed between the United Kingdom and the United States specifically restricts the persons who can be targeted under an order.

20. The Bill sets out three types of orders: law enforcement criminal investigations (Part 2), control order monitoring (Part 3), and national security (Part 4). These are each further divided into three sub-categories relating to purpose: interception, access to stored communications, and access to telecommunications data. This approach preserves the existing structure within the TIA Act and ensures the current safeguards can be applied equally to IPOs (for example, the distinction between category 1 and 2 offences in the Bill).

21. The key aspects of the IPO framework are highlighted below.

***Communications service providers captured by the definition of ‘designated communications providers’***

22. As noted above, the communications landscape and the types of communications service providers have evolved significantly in recent decades. Accordingly, and in recognition of the kinds of international services likely to hold electronic data relevant to Australian criminal matters (such as over-the-top application services like Facebook, Instagram, Skype and Discord), the IPO framework reflects communications technologies in a broad sense. This differs from the current domestic warrant and authorisation regimes for interception, stored communications and telecommunications data access, which are more limited in definition or scope.

23. An IPO can be directed to the following types of CSPs:

- **Carriers and carriage service providers** (e.g. internet service providers and telephone carriers)
- **Message, voice and video call application service providers** (e.g. Facebook Messenger, Skype, WhatsApp)
- **Storage backup providers** (e.g. cloud storage providers)
- **General electronic content providers** (e.g. chat forums, social media platforms and other website providers)

***Types of electronic data that can be sought under an international production order***

24. An IPO can authorise the disclosure of intercepted data, and access to stored communications and telecommunications data. The IPO operates slightly different to an ordinary warrant or authorisation in that it authorises the *disclosure* of electronic data to law enforcement agencies.

25. Sections 7 and 108 of the TIA Act currently prohibit the interception of communications, and the access to stored communications. The *Telecommunications Act 1997* further prohibits the disclosure of telecommunications data. This applies to communications traversing the Australian telecommunications network at the time of interception, or accessing stored communications currently held by an Australian carrier.

26. IPOs will generally apply to disclosure of information held wholly outside of Australia. However, the Bill ensures that where information is held in Australia but the CSP and services are operated offshore but require access to data held in Australia (for example, an Australian data server), they may be able to disclose that data without falling foul of the prohibitions under the TIA Act that would otherwise prevent disclosure.

***Purposes of an international production order***

27. IPOs can only be sought for specific purposes:

- investigating an **offence of a serious crime**:
  - interception – must be for an offence with a maximum penalty of 7 years’ imprisonment or more, or punishable by imprisonment for life, or be captured by the definition of ‘serious offence’ under section 5D of the TIA Act (a serious category 2 offence in the Bill).
  - access to stored communications and telecommunications data – must be for an offence with a maximum penalty of 3 years’ imprisonment or more, or punishable by imprisonment for life (a serious category 1 offence in the Bill).
- **monitoring a person subject to a control order and to detect breaches of the control order**, in addition to monitoring persons to protect the public from terrorist acts, preventing support for terrorist acts and hostile acts overseas, or
- **national security matters**:

- interception and access to stored communications – a person must be reasonably believed to be engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security
- access to telecommunications data – the disclosure must be in connection with the performance of the Australian Security Intelligence Organisation's (ASIO) functions.

### **Agencies that can apply for an international production order**

28. Orders can only be sought by national security and law enforcement agencies who are already able to do so for pre-existing warrants and authorisations under the TIA Act. Specifically, this can be interception agencies, criminal law enforcement agencies, enforcement agencies and ASIO. ASIO will only be able to apply for orders in connection to national security or in connection with the performance of its functions (for orders specifically relating to telecommunications data).

### **The authorisation of international production orders**

29. Those authorised to issue IPOs for law enforcement purposes are broadly consistent with the current warrant frameworks under the TIA Act, with the exception of telecommunications data and national security IPOs.

30. The proposed differences between the pre-existing persons who can authorise warrants and authorisations, and the IPO framework, acknowledges the requirement to adopt a model that best accommodates different legal systems working alongside each other. This generally requires the identification and utilisation of similar decision-makers in approving investigatory powers (such as judicial authorities). Relevantly, the US CLOUD Act requires authorisation of orders by persons characterised as a '*... court, judge, magistrate, or other independent authority*'. The IPO framework facilitates this requirement. Outside of those requirements arising out of international agreements, the current domestic authorisation arrangements for investigatory powers (such as the current warrant frameworks under the TIA Act) strike an appropriate balance between operational needs and appropriately safeguarding individual rights in the domestic context. A breakdown of the differences between the pre-existing persons who can authorise warrants and authorisations and the IPO framework is at **Appendix A**.

31. A range of criteria must be satisfied in order for authorising authorities to approve the order (e.g. reasonable suspicion that a person has committed a serious crime). Authorising authorities must also have regards to a range of other considerations, such as privacy implications, the likely value of the data, and the availability and operational practicalities of other investigatory powers (such as overt search warrants). A comprehensive list of the criteria is at **Appendix B**.

## **Oversight and accountability**

32. Comprehensive oversight and reporting is a key objective of the IPO framework. This has been developed to reflect Australian community expectations of appropriate oversight around the interception of communications, and access to stored communications and telecommunications data under the TIA Act. Core aspects of the oversight and reporting under the IPO framework include:

- Comprehensive oversight regime by the Commonwealth Ombudsman of law enforcement agencies' use of the IPO framework, and the Australian Attorney-General's Department insofar as it relates to its duties as the Australian Designated Authority (see below).
- The Minister, upon receipt of annual inspection reports conducted by the Commonwealth Ombudsman, must cause a copy to be tabled in Parliament.
- Comprehensive oversight regime by the Inspector-General of Intelligence and Security of ASIO's use of the IPO framework (under its existing powers).
- Reporting on ASIO's use of the IPO framework as part of ASIO annual reporting requirements under the *Australian Security Intelligence Organisation Act 1979*.

- Reporting on inspections provided as part of the regular Inspector-General of Intelligence and Security reporting.
33. Furthermore, agencies will only be able to keep sensitive personal communications where there is a legitimate reason to do so; otherwise, agencies will be required to immediately destroy all records obtained using an IPO.

## The requirement for an Australian Designated Authority

34. The Bill sets up an Australian Designated Authority to facilitate key parts of the process. As established by the Bill, the Secretary of the Attorney-General's Department will be the Australian Designated Authority, and may delegate powers and functions to executive level officials within that department. The Australian Designated Authority will:
- review orders for compliance with the nominated designated international agreement and, if an order does not comply, cancel the order and provide advice to the agency that obtained it
  - serve compliant orders, revocations of orders and other notices on designated communications providers
  - receive objections to orders from designated communications providers and
  - in some cases, act as an intermediary between agencies and designated communications providers, by receiving electronic information from designated communications providers pursuant to an order and conveying it to the relevant agency.
35. The Australian Designated Authority will also have a broad discretion to cancel an order at any time. This will ensure that the Australian Designated Authority is able to cancel orders to protect the public interest, or pursuant to any dispute resolution mechanisms in the nominated designated international agreement, or for other reasons. The Australian Designated Authority will be subject to functional oversight by the Commonwealth Ombudsman, and will keep a register of orders issued.

## Enforcement and compliance

36. Enforcement and compliance are key components to any successful investigatory power regime. However, a novel extraterritorial order regime involves conflict of laws issues, which this Bill seeks to overcome.

### *Civil penalty regime*

37. Part 8 of the Bill sets out the enforcement and compliance provisions. This ensures that, to the extent a DCP is capable of complying with an IPO, there is a bona fide tangible outcome for non-compliance., A DCP will be required to meet an 'enforcement threshold' before the relevant enforcement provisions apply (see below).
38. Non-compliance by an individual with an order attracts a civil penalty of 238 penalty units<sup>4</sup>. Non-compliance by a body corporate is up to 200 times that amount<sup>5</sup>. The increase in penalty applicable to body corporates ensures that any penalty for non-compliance by global companies acts as incentive to encourage compliance as necessary.
39. The Communications Access Co-ordinator<sup>6</sup> will be the authorised applicant in relation to seeking civil penalty enforcement in the Federal Court of Australia and the Federal Circuit Court of Australia.

### *Enforcement threshold*

<sup>4</sup> As at 17 March 2020, this amounts to a maximum fine of \$49,980.

<sup>5</sup> Subclause 126(4) sets out the penalty amount for body corporates. As at 17 March 2020, this amounts to a maximum fine of \$9,996,000.

<sup>6</sup> Communications Access Co-ordinator is defined by section 6R of the TIA Act.



40. Clause 125 sets out the requirements where a DCP meets the enforcement threshold (a two-limbed threshold test).

- Firstly, the DCP must provide the relevant service to one or more Australians (or one or more Australians have posted material in terms of a general electronic content service provided by a DCP). This is the ‘*minimum contacts*’ test<sup>7</sup>.
- Secondly, the DCP meets the enforcement threshold **unless** the DCP could not reasonably be considered to have offered or provided the service on the basis of that service being available to Australians.

#### *Utility of the enforcement and compliance provisions under Part 8*

41. The Department of Home Affairs continues to work closely with foreign CSPs to ensure that enforcement is a last resort option, given the practical difficulties inherent in the international context.

## **Evidentiary requirements and admissibility**

42. The IPO framework supports investigation and prosecution of serious crime by applying similar evidentiary certificate regimes that currently exist in the TIA Act.

43. The purposes of evidentiary certificates for IPOs is twofold:

- the protection of capabilities and technologies used to intercept and access electronic data; and
- to reduce the burden on foreign CSP employees being asked to attend court to attest to technical or formal matters and admit records or processes used to produce and subsequently disclose data.

44. There will be five separate types of evidentiary certificates within the IPO framework. These are listed at **Appendix C**.

45. Broadly, these are permitted for DCPs, law enforcement agencies, ASIO and the Australian Designated Authority, and relate to formal or technical matters in terms of actions done to produce or disclose the data in compliance with an order.

46. DCPs will also be permitted to set out facts with respect to acts or things done by the provider to voluntarily provide information in connection with an international production order, including explanatory material or guides as to the operation of their technical systems or processes.

## **Incoming order process – foreign orders and requests**

47. Cross-border access to data agreements are expected to be reciprocal and to require that Australia remove blocking statutes to ensure that Australian industry can disclose electronic data to a foreign authority. Accordingly, under Part 13 of the Bill, Australian industry may comply with a foreign order or request for the disclosure of data, and such compliance will be exempt from:

- the provisions of the TIA Act that prohibit the interception of communications and accessing stored communications;
- the provisions of the TIA Act that prohibit disclosure of that information; and
- the provisions of the *Telecommunications Act 1997* that prohibit the disclosure of information.

48. The Bill also recognises that information disclosed to a foreign authority may be captured by the definition of ‘*personal information*’ for the purposes of the *Privacy Act 1988*. Disclosure of personal information will generally require some kind of authorisation under law. Accordingly, complying with a foreign order or request will be taken to be a disclosure authorised by the TIA Act.

<sup>7</sup> The ‘minimum contacts’ test provides a useful yardstick in considering enforcement and compliance across multiple international jurisdictions.

## Minor amendments

*Redundant references to 'Part 3-3' under section 6DA of the TIA Act definition of 'nominated AAT members'*

49. The Bill does not change who can currently authorise warrants under the TIA Act. However, items 47-49 of the Bill remove a redundant reference to 'Part 3-3' for 'nominated AAT members'. AAT members who have consented to being 'nominated AAT members' for the purposes of section 6DA can only approve interception warrants. AAT members can also be 'issuing authorities' under section 6DB for the purposes of issuing stored communications warrants, and 'Part 4-1 issuing authorities' under section 6DC for the purposes of a journalist information warrant.

50. Accordingly, there is no functional change to AAT members being able to consent to, and receive nominations from the Commonwealth Attorney-General to approve, interception, stored communications and journalist information warrants.

*Substituting the reference to 'Attorney-General' with 'Minister' for extraterritorial operation of warrants under the Surveillance Devices Act 2004*

51. Item 46 of the Bill substitutes the reference to 'Attorney-General' with 'Minister' for extraterritorial operation of warrants under the *Surveillance Devices Act 2004*. The Minister for Home Affairs has administrative responsibility for the *Surveillance Devices Act 2004* and agencies are required to give the Minister evidence in writing that an appropriate foreign official has consented to any surveillance device activities in a foreign jurisdiction.

52. This is in line with amendments made for the extraterritorial operation of computer access warrants introduced as part of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*.

## Consultation

53. The Department of Home Affairs has consulted broadly in developing this legislation, following the commencement of negotiations between Australia and the United States in October 2019 for a bilateral 'CLOUD Act' agreement.

54. This included consultation with Australian agencies who will use and benefit from the IPO framework. Feedback from law enforcement and national security agencies has been vital to ensure the framework is fit-for-purpose and will be effective in combating serious crime.

55. Australian and United States telecommunications providers were also consulted during the development and post-introduction of the legislation. Continued consultation and engagement with these telecommunications providers will be critical to the successful implementation and future operation of the new framework. The private sector is a vital partner in combating serious crime, especially where it relates to criminals taking advantage of communication technologies (such as the internet) and delays caused by current international crime cooperation challenges.

56. Given the interaction with the treaty negotiation process, the Department consulted with the United States Department of Justice on the measures in the Bill.

## Appendix A – Comparison table: Authorising authorities under the international production order framework and the domestic TIA Act framework

International production order authorising authorities		
	Law enforcement orders	National Security orders
<b>Interception</b>	Eligible judges (clause 14) and nominated AAT members (clause 15)	Nominated AAT Security Division member (clause 17) (ASIO must first seek consent of the Commonwealth Attorney-General)
<b>Access to stored communications</b>	Issuing authorities (clause 16) (this includes magistrates, judges and certain AAT members)	Nominated AAT Security Division member (clause 17) (ASIO must first seek consent of the Commonwealth Attorney-General)
<b>Access to telecommunications data</b>	Issuing authorities (clause 16)	Nominated AAT Security Division member (clause 17)
Current TIA Act authorising authorities		
	Law enforcement orders	National Security orders
<b>Interception warrants</b>	Judges (section 6D) and nominated AAT members (section 6DA)	The Commonwealth Attorney-General (section 9)
<b>Access to stored communications</b>	Issuing authorities (section 6DB) (this includes magistrates, judges and certain AAT members)	N/A – access to stored communications currently granted under an interception warrant under section 9
<b>Access to telecommunications data</b>	Authorised officer (section 5AB) (this includes a manager of an enforcement agency or senior executive member of the AFP as authorised by the head of an enforcement agency or AFP Commissioner)	Eligible person (sections 175 and 176)

## Appendix B – Key criteria for authorising an international production order

### *Law enforcement international production orders*

- there are reasonable grounds to suspect that a DCP holds, or is likely to commence to hold relevant data; or
- there are reasonable grounds to suspect that the person is using, or is likely to use, a service;
- obtaining the information would assist in connection with the investigation by the agency of a serious category 1 or 2 offence or offences;
- how much the privacy of any person or persons would be likely be interfered with;
- the gravity of the conduct constituting the serious crime/s;
- to what extent other methods not involving either the interception of communications, or the access to stored communications or telecommunications data are available to the agency;
- how much the use of such methods would assist in the investigation of the serious crime/s;
- how much the use of those methods would prejudice the investigation of the serious crime/s.
- such other matters (if any) as the eligible Judge or nominated AAT member considers relevant.

### *Control order international production orders*

- a control order is in force in relation to the person;
- there are reasonable grounds to suspect that a DCP holds, or is likely to commence to hold relevant data; or
- there are reasonable grounds to suspect that the person is using, or is likely to use, a service;
- how much the privacy of any person or persons would be likely be interfered with;
- how much the IPO would be likely to assist in connection with protection from and prevention of terrorist acts, etc;
- the extent that alternative methods are available, and how much the use of such methods would assist in connection with protection from and prevention of terrorist acts, etc;
- how much the use of those methods would prejudice the protection from and prevention of terrorist acts, etc;
- in the case of interception, whether this would be the method that is likely to have the least interference with any person's privacy.
- such other matters (if any) as the eligible Judge or nominated AAT member considers relevant.

### *National security international production orders*

- that a person is engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security, or
- that a person is using one of the types of services and receiving or sending communications in terms of another person engaged in, or reasonably suspected of being engaged in, or of being likely to engage in, activities prejudicial to security (B-party order);
- that obtaining the data would likely assist ASIO in carrying out its function of obtaining intelligence relating to security;
- The extent other methods that are less intrusive have been used by, or are available to, ASIO;
- how much the use of such methods would likely assist or prejudice ASIO in the carrying out its functions
- such other matters (if any) as the nominated AAT Security Division member considers relevant

## Appendix C - Types of evidentiary certificates for international production orders

### Types of evidentiary certificates for international production orders

Type of evidentiary certificate	Reason for the evidentiary certificate	Conclusive or prima facie evidence of the matters in the document
<b>Designated communications providers evidentiary certificates</b>	A DCP may issue an evidentiary certificate setting out facts with respect to acts or things done by the provider in order to comply with an IPO.	Conclusive evidence
	A DCP may issue an evidentiary certificate setting out facts with respect to acts or things done by the provider to voluntarily provide information in connection with an IPO.	Prima facie evidence
<b>ASIO evidentiary certificate</b>	ASIO may issue an evidentiary certificate setting out facts with respect to the receipt by ASIO of information that was made available to ASIO in accordance with an IPO.	Prima facie evidence
<b>Australian Designated Authority evidentiary certificate</b>	<p>If an IPO requires information to be made available to a law enforcement agency or ASIO indirectly, via the Australian Designated Authority, the Australian Designated Authority may issue an evidentiary certificate setting out facts in respect to:</p> <ul style="list-style-type: none"> <li>the receipt by the Australian Designated Authority of the information; or</li> <li>Anything done by the Australian Designated Authority for the purposes of ensuring that the information was passed on to the agency or ASIO.</li> </ul>	