Australian Government
Department of Home Affairs

Review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

Supplementary Submission

Introduction

1. This supplementary submission, provided to the Parliamentary Joint Committee on Intelligence and Security (the Committee) review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill), addresses matters taken on notice by the Department of Home Affairs (the Department) at the public hearing on 14 May 2020 during the joint appearance of the Department and the Attorney-General's Department. The submission also addresses matters that have arisen in submissions provided to the Committee and that arose during hearings on 12–14 May 2020.
2. The Department's further response at **Appendix C**, addresses written questions on notice provided by the Committee on 20 May 2020.

Consultation on the Bill

3. The Committee sought to understand the nature and extent of the consultation by the Department during the development of the Bill. The Department undertook extensive consultation on the Bill with key Commonwealth agencies, State and Territory government agencies, and the Australian telecommunications industry. This consultation process was productive and assisted in the development of the Bill in its current form.

Consultation with Commonwealth agencies

4. Commonwealth agencies were key stakeholders in the development of the Bill. Early discussions focused on legislative options for supporting a bilateral agreement with the United States on cross border access to data under the United States Clarifying Lawful Overseas Use of Data Act (CLOUD Act).
5. On 7 October 2019, the Minister for Home Affairs and the United States Attorney-General jointly announced the commencement of formal negotiations towards a bilateral Australia–United States CLOUD Act agreement. Following that announcement, the Department began engaging with key Commonwealth stakeholders on a variety of policy proposals to develop an early version of the Bill. The Department circulated discussion papers and held meetings with relevant agencies on a range of core policy issues throughout November and December 2019.
6. Extensive consultation also occurred with the Commonwealth Ombudsman and the Office of the Inspector-General of Intelligence and Security (IGIS). Departmental officials held initial meetings to discuss the proposed legislative framework with the IGIS on 28 November 2019 and with the Commonwealth Ombudsman on 19 December 2019. The meeting with IGIS on 28 November 2019 involved relevant Home Affairs officers up to Senior Executive Service Band 1 and Executive Level 2, while the meeting with the Commonwealth Ombudsman involved Home Affairs officers up to Executive Level 2.
7. Following these meetings, the Department developed a proposal paper for oversight and reporting and circulated to Commonwealth stakeholders including the Commonwealth Ombudsman and IGIS for feedback. Departmental officials also engaged regularly with Commonwealth Ombudsman and IGIS officials by phone and email to obtain feedback and discuss any issues.
8. The Department placed significant weight on feedback from IGIS and incorporated its suggestions into the drafting of the Bill. For example, the provisions in the Bill relating to the following matters are consistent with feedback and views from IGIS during consultation:
    - inclusion of national security international production orders on the general register maintained by the Australian Designated Authority
    - the Australian Security Intelligence Organisation's (ASIO's) record keeping obligations with respect to revocation of orders

- inclusion of requirements for ASIO to destroy certain data when no longer required for a legitimate purpose
- inclusion of requirements for the Attorney-General's prior consent to ASIO applications for orders
- reporting to Ministers and Parliament on IGIS inspections, and
- maintaining the Director-General of Security's ability to personally apply for orders.

The Bill also reflects IGIS' feedback that the Bill did not need to expressly confer powers or functions on IGIS to enable IGIS to oversight ASIO's use of the international production order framework.

9. The Department sought feedback from key Commonwealth agencies on numerous drafts of the Bill and one version of the Explanatory Memorandum. The Department received and incorporated several rounds of feedback from Commonwealth agencies when developing the Bill, and engaged extensively with agencies to understand and respond to issues raised. When provisions were updated, certain agencies received additional versions of the draft Bill that related to their areas of responsibility and interest. A list of key dates is below.

Date	Consultation
1–8 November 2019	Consultation with the Australian Criminal Intelligence Commission (ACIC), Australian Federal Police (AFP), ASIO, AGD, Commonwealth Director of Public Prosecutions (CDPP), Department of Foreign Affairs and Trade (DFAT) and Department of Infrastructure, Transport Regional Development and Communications (DITRDC) on the text of the initial drafting instructions for the Bill.
13 December 2019	Draft Bill circulated to ACIC, AFP and AGD for feedback by 20 December 2019.
7 January 2020	Draft Bill circulated to DITRDC and the Australian Commission for Law Enforcement Integrity (ACLEI) for feedback.
10 January 2020	Revised draft Bill circulated to ACIC, AFP, AGD, CDPP and DFAT for feedback.
13 January 2020	Revised draft Bill circulated to DITRDC for feedback.
16 January 2020	Further revised draft Bill circulated to ACIC, AFP, ASIO, AGD, CDPP and DFAT for feedback by 22 January 2020.
30 January 2020	Further revised draft Bill circulated to ACIC, AFP, ASIO, AGD, CDPP, DFAT, ACLEI, Commonwealth Ombudsman and IGIS for feedback by 6 February 2020.
8 February 2020	Further revised drafted Bill circulated to IGIS.
10 February 2020	Further revised draft Bill circulated to DITRDC.
12 February 2020	OPC circulated draft Bill to AGD, Commonwealth Ombudsman, Office of the Australian Information Commissioner and National Archives of Australia for formal feedback by 14 February.
13 February 2020	Further revised draft Bill circulated to IGIS, AFP, ACLEI, DFAT, Commonwealth Ombudsman and DITRDC for feedback.
17 February	A copy of the revised draft Bill circulated to the Australian Competition and Consumer Commission and the Australian Securities and Investments Commission.
19 February 2020	Further revised draft Bill circulated to CDPP.
6–25 February 2020	Further consultation with individual agencies, including the Commonwealth Ombudsman and IGIS, to resolve outstanding issues and queries in relation to particular measures in the Bill.

27 February 2020	Further revised draft Bill circulated to DFAT. OPC circulated further revised draft Bill to AGD, Commonwealth Ombudsman and National Archives of Australia.
2 March 2020	Final Bill circulated to ACIC, AFP, ASIO, AGD, CDPP, DITRDC, DFAT and the Department of the Prime Minister and Cabinet (PM&C).

Commonwealth senior executive-level interdepartmental steering committee

10. The Department chairs a regular senior executive-level interdepartmental steering committee to discuss and make decisions on matters related to the proposed CLOUD Act agreement with the United States, including the development and intended implementation of the Bill.

11. The committee is comprised of representatives from the Department, Australian Border Force, ACIC, AFP, ASIO, AGD, CDPP, Department of Finance, DFAT, DITRDC and PM&C. Occasionally, there may be observer agencies.

12. These committee meetings have been held regularly since January 2019 and will continue through the establishment of the Bill and proposed CLOUD Act agreement. The proposed legislation was a key focus of discussion at four meetings prior to introduction of the Bill held on 25 October 2019, 19 November 2019, 22 January 2020 and 14 February 2020.

State and Territory consultation

13. State and Territory agencies will be a significant adopter of the international production order framework. The Department has consulted extensively with State and Territory governments on the Bill.

14. Engagement with State and Territory agencies on the legislation commenced at the Interception Consultative Committee meeting on 29 October 2019. The Interception Consultative Committee is an established forum chaired by the Department that includes representatives of Commonwealth and State and Territory government agencies that are able to obtain interception information. Also present at this meeting were representatives from the Australian telecommunications industry. At the meeting on 29 October 2019, a departmental senior executive officer, briefed State and Territory representatives on the proposed CLOUD Act agreement and commenced discussions on necessary legislative reform and the impact on Australian industry.

15. In December 2019, the Department contacted the State and Territory members of the Interception Consultative Committee to confirm the appropriate agencies and contacts for consultation on the Bill. Based on this feedback, the following agencies were consulted through the development of the Bill:

State	Agencies consulted
New South Wales (NSW)	NSW Police Force Department of Communities and Justice Independent Commission Against Corruption Law Enforcement Conduct Commission NSW Crime Commission
Victoria	Victoria Police Department of Premier and Cabinet (including the Public Interest Monitor) Independent Broad-based Anti-corruption Commission
Queensland	Queensland Police Service Department of Justice and Attorney-General (including the Public Interest Monitor) Crime and Corruption Commission
Western Australia	Western Australia Police Force Corruption and Crime Commission

	Department of Justice Department of the Premier and Cabinet
South Australia	South Australia Police Independent Commissioner Against Corruption Department of Premier and Cabinet
Tasmania	Tasmania Police Department of Police, Fire and Emergency Management
Northern Territory (NT)	NT Police, Fire, and Emergency Services
Australian Capital Territory (ACT)	ACT Policing Justice and Community Safety Directorate

16. In January 2020, departmental officials held teleconferences with all States and Territories (except the ACT) on the progress of the CLOUD Act agreement negotiations and the development of the legislation. These teleconferences provided an opportunity for discussions as to the purpose and intent of the legislation, and the development and intended operation of specific measures. Teleconferences were held on the following dates:
    - **Queensland:** 10 January 2020
    - **New South Wales:** 13 January 2020
    - **Northern Territory:** 13 January 2020
    - **Victoria:** 14 January 2020
    - **Western Australia:** 17 January 2020
    - **South Australia:** 21 January 2020, and
    - **Tasmania:** 22 January 2020.
17. The Department also offered to meet with ACT Government agencies, and circulated fact sheets to all States and Territories setting out core concepts and measures to be included in the Bill.
18. The Department circulated the draft Bill to State and Territory agencies on 7 February 2020, followed by a revised draft on 14 February 2020 that incorporated feedback. These exposure drafts gave agencies the opportunity to gain a deeper understanding of the intricacies of the Bill and to provide considered feedback for the Department's consideration. Feedback provided on the exposure draft primarily related to the exceptions for use and disclosure of protected information and evidentiary certificates.
19. During this process, States and Territories were also encouraged to consider whether any amendments would be required to State and Territory legislation to support their adoption of the international production order framework.
20. Departmental officials met with NSW Police in Sydney on 21 February 2020 to consult on the proposed CLOUD Act agreement and legislation in detail. As NSW Police is expected to be a key user of the international production order/CLOUD Act agreement framework, this meeting was valuable to build understanding of how the framework will operate, including its key safeguards and limitations, and to address concerns and questions.

Industry consultation

21. Engagement with Australian industry also commenced at a special industry-government day meeting held by the Interception Consultative Committee on 29 October 2019. During that meeting, industry participants were briefed on the Government's intention and preparations for the proposed CLOUD Act agreement with the United States, potential options for legislative reform, and possible impacts on Australian industry.

During this meeting it was agreed that an industry working group would be set up to ensure engagement with industry as required.

22. The industry working group comprises the following Australian companies:
    - Telstra;
    - Vodafone;
    - Optus;
    - TPG;
    - NBN Co; and
    - Vocus.
23. The Department led industry working group meetings on 6 November 2019 and 16 January 2020, which involved further detailed discussions on a CLOUD Act agreement and the development of implementing legislation. Feedback, questions and concerns from industry in these meetings were all taken into consideration in developing the legislation.
24. On 12 and 13 February 2020, departmental officials provided industry working group members with two full-day briefing sessions in Melbourne and Canberra to view and provide comments on the draft Bill. Vocus, Telstra, Optus and NBN Co attended in response to the offer. DITRDC also attended the Canberra session. During these sessions, industry asked questions related to compliance, impact of the new regime and its practical functions. Definitions and policy intentions behind portions of the Bill were explained.
25. In response to a request by industry to clearly distinguish the parts of the Bill relevant to foreign providers compared with Australian providers, the part of the Bill titled 'Incoming orders and requests' was moved from part way through the Bill to near the end of the Bill (as Part 13). Also upon request from industry, a detailed explanation of the definition of *interception* was included in the Bill's Explanatory Memorandum.
26. The Department has also engaged with Fastmail, an Australian email service provider that has previously received mutual legal assistance requests from foreign countries. A departmental senior executive officer and official travelled to Melbourne to meet with Fastmail on 25 November 2019 to provide information on the US CLOUD Act and planning for the legislation. Departmental officials also provided Fastmail a confidential briefing session in Melbourne on 12 February 2020 to review and provide feedback on the draft Bill.
27. On 25 February 2020, the Department briefed the Communications Alliance, and participating industry members, on the CLOUD Act agreement and proposed legislation. The briefing was provided by a departmental senior executive officer and supporting officers.

Other consultation

28. The Department also consulted with the United States Department of Justice to ensure that the international production order framework met the requirements of the CLOUD Act.

Departmental responses to recommendations in the Inspector-General of Intelligence and Security submission

29. As requested by the Committee, the Department has provided a written response to each of the recommendations made by IGIS in its public submission at **Appendix A**.
30. Consultation with IGIS related to their role of overseeing the functions of ASIO with respect to the powers and obligations conferred on ASIO by the Bill. Accordingly, while not all of IGIS' recommendations were

accepted during consultation, the Department considers that consultation with IGIS was productive and assisted the Department to shape the policy underpinning the oversight of ASIO's functions under the Bill. We understand that IGIS further reflected on the Bill after introduction and provided additional feedback by way of their submission.

Comparison of offence thresholds in the TIA Act and the Bill

Current domestic framework

31. The *Telecommunications (Interception and Access) Act 1979* (TIA Act) sets out specific offence thresholds for each access regime that must be met prior to accessing data for law enforcement purposes. These access regimes are interception, access to stored communications, and access to telecommunications data. Broadly, these thresholds are the following:

- Interception – '*serious offence'* threshold – defined in section 5D of the TIA Act to include certain offences punishable by a maximum term of imprisonment of at least 7 years or life, and certain other offences below that penalty threshold.
- Stored communications access – '*serious contravention'* threshold – defined in section 5E of the TIA Act to include an offence punishable by a maximum term of imprisonment of at least 3 years, offences carrying certain pecuniary penalties, or a '*serious offence'* for which an interception warrant could be sought.
- Historical telecommunications data access:
  - enforcement of the criminal law, or
  - enforcement of a law imposing a pecuniary penalty or protection of the public revenue.
- Prospective telecommunications data access:
  - a '*serious offence'*, or
  - an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

International production order framework

32. The offence thresholds for obtaining international production orders related to law enforcement under Part 2 of the Bill are closely modelled on the existing offence thresholds in the TIA Act and have been tiered so that the most intrusive access regime (interception) is tied to the most serious threshold offences. The Bill was not able to adopt identical thresholds to that in the TIA Act for stored communications and telecommunications data in order meet international expectations. For example, under the United States CLOUD Act, foreign orders subject to a CLOUD Act agreement must be for the purpose of preventing, detecting, investigating or prosecuting serious crimes that are punishable by a penalty of three years' imprisonment or more.

33. The thresholds are as follows:

- Interception – '*serious category 2 offence*' – punishable by imprisonment for at least 7 years, or is otherwise included in section 5D of the TIA Act (includes excepted offences);
- Stored communications - *'serious category 1 offence*' – a criminal offence punishable by imprisonment for at least 3 years; and

- Telecommunications data - *'serious category 1 offence*' – a criminal offence punishable by imprisonment for at least 3 years.

34. A comparison table of the law enforcement thresholds is provided at **Appendix B.**

Ministerial guidelines

35. Under section 8A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), ASIO must conduct its security intelligence activities in accordance with Ministerial guidelines. The guidelines stipulate that ASIO must conduct its activities in a lawful, timely and efficient manner while applying the principle of proportionality to ensure the least intrusion necessary into an individual's privacy. ASIO's use of the international production order framework will be governed by the Ministerial guidelines.

36. The Department is preparing revised guidelines for consideration by the Minister of Home Affairs. This has involved extensive and close consultation with both ASIO and IGIS. Approval and timing for the release of the revised guidelines is a matter for the Government.

ONI Assessment Consultation Board

37. The Department has referred the matter to ONI for response.

Appendix A – Departmental responses to IGIS submission

Topic	Matters for consideration	Response
Threshold issues	***Differing authorisation standards between international production orders and existing ASIO warrants*** The differences between the authorisation framework for the proposed international production order framework and ASIO's existing warrant framework, and between international production orders in relation to telecommunications data and international production orders in relation to interception and stored communications, invite the Committee's consideration (IGIS submission, p. 7).	As noted in the table at Appendix A to the Department's preliminary submission to the Review, under Part 4 of the Bill, all international production orders sought by ASIO must be independently authorised by an Administrative Appeals Tribunal (AAT) Security Division member. This differs from the domestic framework in the TIA Act, under which ASIO warrants for interception or stored communications are authorised by the Attorney-General, ASIO journalist information warrants for telecommunications data are authorised by the Attorney-General, and authorisations for telecommunications data can be internally authorised. There is a clear policy reasoning for the different authorisation mechanism adopted for ASIO in the Bill, which reflects the unique requirements of the United States CLOUD Act. It is imperative that the framework of international production orders is well-placed to work alongside many different foreign legal systems. For example, the United States CLOUD Act requires that foreign orders under CLOUD Act agreements must be subject to review or oversight by an authority characterised as a "court, judge, magistrate, or other independent authority". The importance of the Attorney-General's longstanding role in terms of ASIO's powers to seek interception and access to stored communications is maintained in the Bill. Under Part 4 of the Bill, ASIO can only make an application to a nominated AAT Security Division member for an interception or stored communications international production order if ASIO has obtained the Attorney-General's prior consent to the application being made. The different authorisation mechanism adopted for this legislation does not reflect any change in policy regarding the appropriateness of the existing domestic warrant processes under the TIA Act.
	Statutory requirement to consider privacy and proportionality The Committee may wish to consider a statutory requirement for nominated members of the Security Division of the AAT to consider privacy, proportionality and human rights in deciding whether to issue any of the three categories of international production orders that may be sought in relation to national security (IGIS submission, p. 8).	The criteria that must be considered by a nominated AAT Security Division member before issuing a national security international production order under Part 4 of the Bill recognises ASIO's role as being anticipatory and protective in nature. In issuing domestic warrants to ASIO for interception and stored communications, the Attorney-General is required to consider criteria relating to the person's suspected engagement in activities prejudicial to security, and the likely value of the information being sought to ASIO's carrying out of its functions. Different thresholds apply to different types of warrants. Similar criteria are applied in the Bill and the Attorney-General must consider these in order to consent to a national security international production order for interception or stored communications. The additional criteria which must be considered by a nominated AAT Security Division member to authorise an international production seeks to ensure that the international production order framework works effectively with the proposed CLOUD Act agreement and other future agreements. For example, a key

Topic	Matters for consideration	Response
		requirement under the United States CLOUD Act is the requirement that consideration be had to the availability of less intrusive methods than the kind of surveillance being requested. Specifically, the criteria provided for national security international production orders require various considerations that go to an overall calculus of whether the order would be proportionate, reasonable and necessary in the circumstances. For example, each order requires consideration of the following (amongst other things): • To what extent methods of carrying out ASIO's function of obtaining intelligence relating to security that are less intrusive than the kind of investigative activities being requested (interception, access to stored communications or telecommunications data) have been used by, or are available to ASIO. • How the use of those methods would likely assist ASIO in carrying out its function of obtaining intelligence relating to security. • How much the use of those methods would likely prejudice ASIO in carrying out its function of obtaining intelligence relating to security. • Such other matters (if any) as the nominated AAT Security Division member considers relevant. The decision-maker is also able to take into consideration any other matters they consider relevant, which may include further privacy or human rights considerations. These additional criteria ensure that the nominated AAT Security Division member assesses the potential privacy impacts, and that the proposed interference with privacy is proportionate to the national security purpose. *Ministerial guidelines in relation to ASIO* Under section 8A of the ASIO Act, ASIO is required to comply with Ministerial guidelines. The Guidelines ensure that privacy, proportionality and human rights are considered in issuing ASIO warrants under the TIA Act, and the Guidelines will also apply to national security international production orders. The guidelines provide that information to be obtained by ASIO is to be done in a lawful, timely and efficient way and in accordance with the following: • any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence

Topic	Matters for consideration	Response
		• inquiries and investigations into individuals and groups should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions, and • wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques. These considerations ensure that ASIO conducts a thorough assessment of the potential privacy impacts before seeking to use covert powers such as those under an international production order, and that the use of those powers, including the necessary interference with a person's privacy, are proportionate to the relevant conduct. Noting these requirements it is unnecessary and duplicative to replicate them in the Bill.
	Threshold for applying for an international production order in relation to telecommunications data Given that the informative value and relative privacy intrusion of the data has increased significantly with technological advances, the Committee may wish to consider the threshold for applying for an international production order for telecommunications data (IGIS submission, p. 9).	The threshold for ASIO to apply for an international production order relating to telecommunications data is that the use of such methods would be likely to assist ASIO in performing its functions. This is in line with the threshold for domestic telecommunications data authorisations for ASIO. The decision to maintain this threshold was made to provide ASIO with the operational flexibility and consistency it needs to carry out its functions, whilst balancing it with additional criteria the nominated AAT Security Division member must consider. As with all ASIO intelligence activities, consideration in applying for, granting access to, and handling telecommunications data and intercepted or stored communications data will be consistent with ASIO's internal policies and procedures and the Ministerial Guidelines. ASIO will ensure that the approval levels for international production orders are aligned as closely as possible with approval levels in ASIO's existing framework.
	Update on Attorney-General's Guidelines The Committee may wish to seek an update on the revision of the ASIO Guidelines. IGIS supports the ASIO Guidelines being comprehensively updated, in consultation with this office, as a matter of priority (IGIS submission, p. 10).	The Department acknowledges the change to the technological environment, ASIO's statutory powers and the need to update the Ministerial Guidelines in relation to ASIO. The Department has completed a review of the existing Attorney-General's guidelines relating to ASIO and is now in the process of preparing revised guidelines for the consideration of the Minister for Home Affairs. The Department has worked closely with IGIS and ASIO to ensure that the revised Guidelines are fit for purpose in the current environment, including providing guidance in relation to ASIO's access to and retention of personal information.
	Extending additional protections that apply to existing communications access	The journalist information warrants under the TIA Act provide an additional layer of protection telecommunications data relating to journalists' sources. An independent authorisation by a decision-maker

Topic	Matters for consideration	Response
	The Committee may wish to consider whether the protections afforded to certain groups under Australia's domestic authorisation scheme, as well as the protections for other privileges, should apply to the proposed international production order scheme. If so, the Committee may wish to consider amendments that require an issuing authority to consider additional matters in relation to certain groups.	outside of the agency will issue the warrant, rather than the typical process of internal authorisation by agencies for telecommunications data. However, our domestic interception and stored communications warrants do not include these particular carve-outs as they are already subject to independent authorisation. Exemptions may also raise issues associated with the application of investigatory powers on the basis of profession-based carve-outs and present challenges for agencies in investigating matters relating to crime or national security. In addition to legislative safeguards, there will be governance and accountability mechanisms, such as ministerial directions under subsection 37(2) of the *Australian Federal Police Act 1979*. In August 2019, the Minister for Home Affairs issued a Ministerial Direction outlining the Government's expectations for the AFP in relation to investigative action involving a professional journalist or news media organisation in the context of an unauthorised disclosure of material made or obtained by a current or former Commonwealth officer.
Application process	*Limitations on who may apply for an international production order* The Committee may wish to consider whether the Bill should be amended to reflect ASIO's domestic telecommunications warrant framework so as to limit authority to apply for an international production order to the Director-General of Security. If a limited delegation power was considered necessary, the Committee may wish to consider limiting delegations to a Deputy Director-General or Deputy Directors-General.	The Department acknowledges this is partly different to the current domestic ASIO warrant framework. *Current interception warrant approach* Currently only the Director-General of Security can apply to the Attorney-General for interception warrants to the Attorney-General (stored communications access is authorised under an interception warrant). This is currently not delegable. *Telecommunications data approach* Telecommunications data access is authorised internally by an 'eligible person' who is: • the Director-General of Security; or • a Deputy Director-General of Security; or • an ASIO employee or ASIO affiliate covered by an approval from the Director-General of Security.

Topic	Matters for consideration	Response
		Delegation for an application under the Bill The Bill provides for a flexible delegation across all three types of national security international production orders. Those who can apply are the following: • the Director-General of Security; or • a Deputy Director-General of Security; or • an ASIO employee in relation to whom an authorisation is in force. This approach to delegation would provide ASIO with flexibility to determine who is operationally best placed and qualified to make an application for a national security international production order. For example, requiring the Director-General of Security or a Deputy Director-General of Security to make applications for a telecommunications data international production order would require them to potentially make hundreds of applications, appearing personally before the AAT Security Division member. While this appears to be different to the domestic ASIO warrants, this is in line with the approach taken for law enforcement domestic warrants and international production orders that provide a broad flexible delegation for the head of the agency to determine who is best placed to apply for warrants/orders. As with all ASIO intelligence activities, consideration in applying for, granting access to, and handling telecommunications data and intercepted or stored communications data will be consistent with ASIO's internal policies and procedures and Ministerial guidelines. ASIO will ensure that the approval levels for international production orders are aligned as closely as possible with approval levels in ASIO's existing framework.
	'Urgent Circumstances' The Committee may wish to consider including statutory guidance on what will constitute 'urgent circumstances' for the purpose of a telephone application. In any event, an amendment to provide that the particulars of the urgent circumstances which necessitate making a telephone application be communicated to the Attorney-General when seeking the	ASIO must provide particulars of why the urgent circumstances mean it is necessary to make the application by telephone to the nominated AAT Security Division member who authorises the application (for example, see clause 87 and paragraph 89(2)(d) for interception national security international production order). To ensure accountability for urgent telephone applications, a report must be provided to the Attorney-General that sets out: • the particulars of the urgent circumstances because of which the person thought it necessary for the Attorney-General to consent orally; and • whether the application was granted, withdrawn or refused.

Topic	Matters for consideration	Response
	Attorney-General's oral consent would assist the Attorney in considering the application.	This must be done within 3 working days after the day on which the application was granted, withdrawn or refused. A copy of that report must be provided to the Inspector-General of Intelligence and Security within that same period. In addition to reporting requirements above, the Department notes that telephone applications form only a small per cent of the applications made each year for the domestic regime. As noted in the evidence provided by the Department on 14 May to the Committee, in the 2018-2019 financial year, approximately: • 1.3 per cent of intercept applications were made by telephone for urgent applications. • 0.08 per cent of stored communication warrants were made by telephone for urgent applications. In terms of the need for statutory guidance in the legislation, the Department notes that as currently drafted it relies on its ordinary meaning and is intended to cover circumstances which because of their urgency, mean that it is not possible to make an application in writing in the normal way following normal processes. While this power is unlikely to be used often, it is important that the legislation does not seek to anticipate every potential scenario where it may be needed because of 'urgent circumstances'. To do so may limit the operational utility of the regime.
Reporting and transparency	*Extending Attorney-General reporting requirements* The Committee may wish to consider (a) extending the requirement to report to the Attorney-General to all international production orders; and (b) whether the matters on which ASIO is required to report to the Attorney-General should be expanded.	Clause 129 of the Bill requires a report to be made to the Attorney-General for each international production order issued under clause 89 (interception) within 3 months subject to a range of factors, (e.g. the last day the DCP could have done an act or thing in compliance with the order). This reporting requirement reflects the domestic ASIO warrant framework (section 17). The policy reasoning for this was based on interception being considered the most intrusive type of international production order according to the TIA Act. Given the likely amount of telecommunications data international production orders, it would place a high administrative burden on ASIO to provide a report on each single telecommunications data international production order. Accordingly, a different approach would be required to balance accountability and transparency with how best to meaningfully report to the Attorney-General for these orders.
	Publication of statistics in annual report The Committee may wish to consider whether it would be appropriate to require statistical reporting on ASIO's use of the international production order framework to be made public.	ASIO is not currently required to include statistical reporting on its use of the TIA Act in its public annual report.

Topic	Matters for consideration	Response
	Tabling designated international agreements. The Committee may wish to seek assurance that designated international agreements entered into under the framework established by the Bill will be made public.	Yes, designated international agreements, including any amendments to these agreements, would be made publically available through the usual parliamentary processes and publication in treaty databases. It is normal practice that bilateral treaties are confidential between the parties until the treaty has been signed, unless both parties agree to earlier disclosure. After signing, all treaties must be tabled in Parliament to facilitate public consultation and parliamentary scrutiny. Under Article 102 of the Charter of the UN, any Treaty that comes into force must be registered with and published by the UN. Additionally, the designated international agreements as treaties will also be published in the Australian Treaties Database and Australian Treaties Library.
Destruction of data	*Statutory requirement for periodic review of the relevance of data collected under international production orders* A statutory requirement that ASIO periodically review the relevance of data collected under international production orders would give effect to the Bill's requirement that, where the Director-General of Security is satisfied that the information is not likely to be used for a relevant purpose, the record must be immediately destroyed. The Committee may also wish to consider whether the Director-General's obligations in this regard should be delegable and whether the destruction obligations should be extended to telecommunications data provided under an international production order (in addition to intercepted and stored communications).	<u>Statutory requirement for periodic review</u> The destruction requirements in the Bill mirror those in the TIA Act. Clause 140 of the Bill places an obligation on agencies to destroy records of intercepted and stored communications obtained under an international production order when it is no longer required for a legitimate purpose referred to in clauses 153, 157 or 158. Comprehensive oversight of agencies' compliance with this requirement will be provided by the Commonwealth Ombudsman and IGIS. <u>Extending destruction requirements to telecommunications data international production orders</u> Consistent with current arrangements under the TIA Act, the Bill does not include a destruction requirement for telecommunications data obtained under an international production order. Agencies must have the ability to retain telecommunications data for a sufficient period of time as the information it provides may facilitate their efforts to keep the community safe. Telecommunications data obtained at a point in time or in relation to a specific investigation may provide important evidence and intelligence that assists agencies in developing an understanding of criminal and terrorist networks. ASIO will continue to work within the framework provided by the National Archives legislation and the Ministerial guidelines in relation to the disposal of records.

Topic	Matters for consideration	Response
Notifications, access and record keeping	*General notification obligation with timing able to be varied administratively* The Committee may wish to consider a statutory obligation in the Bill for ASIO to notify the IGIS of all international production orders that are issued within three months, with the option to vary the notification periods by agreement between the Inspector-General and the Director-General of Security.	ASIO and IGIS would be able to set notification periods administratively for national security international production orders. This would allow for flexibility given the uncertain number of requests until the international production order framework is operational. This approach was previously discussed with both the Office of the IGIS and ASIO as there were concerns from the Department that hundreds of notifications going through a single mechanism may result in increased administrative burden on the Office of the IGIS and not result in meaningful oversight. With that in mind, no major concerns were identified by the Office of the IGIS and ASIO.
	Statutory authority to access register held by Australian Designated Authority The Committee may wish to consider amendments to provide express authority for the IGIS to access the register of international production orders kept by the Australian Designated Authority, to the extent that the register relates to international production orders issued in relation to national security.	This was not included in the Bill as the Australian Designated Authority may already share information with the IGIS for the performance of their oversight of the international production order framework in so far as it relates to ASIO.
	Robust record retention requirements The Committee may wish to consider the duration of the obligation to retain records, and whether all information and documents prepared for the operation of the regime should be statutorily required to be kept for IGIS inspection.	The approach in the Bill was modelled on the law enforcement legislative requirements under the TIA Act. See for example, subsection 151(3) of the TIA Act. ASIO does not have an equivalent provision.
	Amendments to secrecy provisions	The exceptions in Part 11 of the Bill were crafted to ensure that information could be used and disclosed appropriately for the purpose of an IGIS official exercising a power, or performing a function or duty, as an

Topic	Matters for consideration	Response
Technical matters	The Committee may wish to consider: • an amendment to clause 153 to enable international production order information to be used, recorded or disclosed for the purpose of 'an IGIS official exercising a power, or performing a function or duty, as an IGIS official'. • an amendment to the IGIS Act to provide explicit authority for IGIS officials to share information with the Attorney-General's Department for the purpose of its role as Australian Designated Authority.	IGIS official. The inclusion of the reference to IGIS' legislation in subclause 153(1)(p) is intended to ensure that the exception is broad enough to include functions or powers applicable to IGIS more broadly as contemplated under its legislation. The same consideration was adopted in relation to the exception relating to the Commonwealth Ombudsman in subclause 153(1)(q).
	Consistency of definitions Different definitions for the same terms may cause complexity and result in confusion in the proposed new international framework.	The definitions in the Bill were crafted on the advice of experienced drafters from the Office of Parliamentary Counsel.

Appendix B

Comparison table: Offence thresholds under the TIA Act and the Bill		
	Offence threshold for domestic warrants and authorisations in the TIA Act	**Offence threshold for International Production Orders for enforcement of the criminal law (Part 2 of the Bill)**
Interception	A '*serious offence*' is defined in section 5D, and includes certain offences punishable by a maximum term of imprisonment of at least 7 years or life, and certain other offences below that penalty threshold.	A '*serious category 2 offence'* is defined as a '*serious offence'* as set out in section 5D of the TIA Act, or an offence that is punishable by a maximum term of imprisonment of 7 years or more, or life' (clause 2).
Stored communications	A '*serious contravention'* is defined in section 5E, and includes an offence punishable by a maximum term of imprisonment of at least 3 years, offences carrying certain pecuniary penalties, or a '*serious offence'* for which an interception warrant could be sought.	A *'serious category 1 offence'* is defined as an offence that is punishable by a maximum term of imprisonment of 3 years or more, or life (clause 2).
Telecommunications data	For historical data: '*reasonably necessary for the enforcement of the criminal law'* (section 178(3)), finding a missing person, enforcing a law imposing a pecuniary penalty or protecting the public revenue. For prospective data: '*reasonably necessary for the investigation of a serious offence (for which an interception warrant could be sought) or an offence…that is punishable by imprisonment for at least 3 years'*	A *'serious category 1 offence'* is defined as an offence that is punishable by a maximum term of imprisonment of 3 years or more, or life (clause 2).

Appendix C: Responses to written questions on notice

This further response, provided to the Parliamentary Joint Committee on Intelligence and Security (the Committee) review of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (the Bill), addresses written questions on notice provided by the Committee on 20 May 2020.

Question on Notice – Consultation with the US (Home Affairs)

1. Has the Department consulted with US stakeholders about this Bill to ensure that it meets US requirements (around human rights/privacy/third country liabilities)?

The Department of Home Affairs (the Department) has engaged with the United States Government regularly throughout the development of the Bill to ensure that the framework will meet the requirements under the United States Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

a) Who has the Department consulted with, when and in what detail?

The Department engages regularly with the United States Department of Justice to discuss the proposed CLOUD Act agreement between Australia and the United States and the Bill. The United States Department of State has also attended some discussions at the invitation of the Department of Justice.

The Bill was discussed at a senior level with the United States Department of Justice during the second round of negotiations on the proposed CLOUD Act agreement held in Sydney from 19–21 February 2020.

b) Were any concerns raised? If so, what were they?

The content of bilateral discussions with the United States are confidential pursuant to a Memorandum of Understanding between the United States and Australia.

c) Are you aware of any other agencies (i.e. Attorney Generals) that may have also consulted with US counterparts? If so, with whom and when?

Representatives from the Attorney-General's Department and the Department of Foreign Affairs and Trade participated in the second round of negotiations on the proposed CLOUD Act agreement from 19–21 February 2020. In addition, both the Attorney-General's Department and ASIO have participated in meetings or teleconferences with the United States Department of Justice, led by the Department.

2. Are any agencies or departments in the United States that have, or will, view a final version of the Bill to ensure its compatibility with the CLOUD Act? Who, on what dates and what specific concerns, if any, have they raised?

A key requirement for the United States Government, before it will sign a CLOUD Act agreement with Australia, is that Australian law and the proposed agreement comply with the requirements of the United States CLOUD Act. We anticipate that after the final Bill is finally passed, the United States Attorney-General will consider whether to certify that Australian law, including the Bill as passed, complies with the CLOUD Act requirements. As stated above, the Department has liaised extensively with the United States Department of Justice during the development of the Bill to ensure that it will comply with the CLOUD Act requirements.

3. Has the US (i.e. DOJ or others) raised any concerns at any point over the Assistance and Access Act and its interplay with this Bill?

On 4 October 2019, Jerrold Nadler, Chairman of the United States House of Representatives Committee on the Judiciary, wrote to the Minister for Home Affairs seeking clarification to ensure that the Assistance and Access Act would not undermine the ability for Australia to qualify for an executive agreement under the CLOUD Act with the United States. The Minister responded in detail to Chairman Nadler's letter and the Department has worked closely with the United States Department of Justice to clearly explain the operation of the Assistance and Access Act. In response to this engagement, the United States Department of Justice has confirmed that there are no issues with the Assistance and Access Act that would prevent Australia from successfully negotiating a CLOUD Act agreement with the United States, including in its April 2020 submission to the Committee's review of the Assistance and Access Act.

4. Is the Department aware of any concerns in the US Government or US Congress over the provisions in this Bill or its compatibility with the CLOUD Act? If so, please provide details.

Please see response to question 3.

Question on Notice – ASIO Guidelines (Home Affairs)

1. On what date did Home Affairs receive ASIO's draft revised guidelines from ASIO for review?

There has been an ongoing process of consultation and revision between the Department, ASIO and IGIS of the 2007 ASIO Guidelines.

Most recently, the IGIS provided extensive feedback in late-November 2019, after which the Department, IGIS and ASIO worked to further update the Guidelines. ASIO provided further comments on the draft revised Guidelines to Home Affairs on 13 May 2020.

2. Who in the Department received it?

Officers in the National Security Policy Branch of the Department received comments from ASIO on 13 May 2020.

3. What other agencies is the Department required to, or wanted to, consult with on the draft guidelines? In the IPO hearings, ASIO noted Attorney Generals, and Home Affairs noted IGIS. Are there other agencies that have been consulted as required or as a courtesy?

In addition to ASIO and IGIS, the Attorney-General's Department and the Office of the Australian Information Commissioner were consulted on the revised Guidelines and provided feedback to Home Affairs. Suggestions made by these agencies were incorporated to the extent possible. It is important to note, that the Minister for Home Affairs is required to consult the Attorney-General before issuing the revised Guidelines.

a) On what date/s were the draft guidelines sent from Home Affairs to IGIS or other agencies for consultation? (agency and date)

There has been extensive consultation between the Department and IGIS over the course of the review of the Guidelines. Since January 2020, the Department has circulated three revised versions of the Guidelines to ASIO and the IGIS for comment.

b) How much time was allowed for each response? (agency and date)

Please see responses to questions 1 and 3(a).

4. Were all suggested comments or amendments from other departments incorporated? If not, why not and which ones? Please provide detail on all suggested changes.

Please see response to question 3.

5. When will the guidelines be released?

Please see Appendix A at pages 11-12.

a) Does the Minister have to approve the guidelines? Will he in this instance?

Yes.

b) Is the Minister's approval required from a timing or substance perspective (as alluded to in the hearings)?

The Minister for Home Affairs is responsible for issuing any Guidelines to ASIO pursuant to section 8A of *the* ASIO Act. While the Department works with relevant agencies to develop the revised Guidelines, substance and timing is a matter for Government.

Questions on notice – International Production Orders Bill – Department of Home Affairs and Attorney-General's Department

In terms of the questions on the IPO Bill, the Department has not responded to the questions posed on the Government's response to the recommendations. This is a matter for Government.

1. **The Law Council recommends that the Government provide public assurances that "the Australian Treaty Making Process, including the existing arrangements for Parliamentary scrutiny by JSCOT, will apply to all agreements made by Australia with foreign countries that are intended to be prescribed as DIAs in regulations made under Clause 3 of proposed Schedule 1 to the TIA Act".**

   a) What is the Department's response to this recommendation?

The Department confirms that all international agreements to be designated for the purposes of the international production order framework will be subject to Australia's treaty-making requirements, including tabling in Parliament. As noted in the Department's public hearing evidence to the Committee on 14 May, such requirements would also include scrutiny by the Joint Standing Committee on Treaties. The requirements of the treaty-making process will also apply to any proposed amendment to a designated international agreement.

   b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 1(a) above.

2. **The Law Council recommends that clause 3 of proposed Schedule 1 to the TIA Act be amended "to provide that the regulations prescribing an agreement between Australia and a foreign country, or countries, as a DIA must reproduce the relevant agreement in full (for example, as a schedule)".**

   a) What is the Department's response to this recommendation?

Clause 3 of the Bill only requires that the name of the agreement be specified in the regulations. While this was a policy proposal by the Department, the Department notes that Office of Parliamentary Counsel Drafting Direction No. 3.11 states that, while reproducing the text of an international agreement "is convenient for the reader", "it can involve a lot of work in obtaining the authoritative text of the treaty, formatting it and checking it" and "since international agreements are now ordinarily available on the internet, it is probably less important for legislation to include the text of agreement."

All international agreements, including amendments to designated international agreements, will be made publicly available through, for example, parliamentary processes and publication in the Australian Treaties Database.

   b) What are the likely consequences / implications of implementing this recommendation?

Implementing this Law Council recommendation would mean the text of the agreement in the regulations would need to be updated each time an agreement is amended, extended or renewed for a further period, and steps will need to be taken to ensure the commencement of the new regulations aligns with the commencement of the new agreement. If this does not occur, this could lead to uncertainty about the status of international production orders that have already been issued or that are in force before the updated regulations (and updated agreement) commence. The risk of uncertainty could be greater if the recommendations referred to in questions 3 and 5 below were also to be adopted. In addition, a legislative requirement for the text of multiple treaties to be set out in a single set of regulations may lead to large, unwieldly regulations.

3. **The Law Council recommends that proposed Schedule 1 to the TIA Act be amended "to provide that regulations made under Clause 3 (listing an agreement as a DIA) do not commence until after the statutory disallowance period for those regulations under the Legislation Act 2003 (Cth) has expired".**

    a) **What is the Department's response to this recommendation?**

Subclauses 3(1) and (3) of the Bill provide that an agreement is not a 'designated international agreement' for the purposes of the framework unless the name of the agreement has been specified in the regulations and it has entered into force. As a matter of practice, the Department would not normally advise a foreign country that Australia has completed all steps required for an agreement to enter into force until the parliamentary disallowance period for implementing regulations has ended. It is anticipated that this practice will be followed for international agreements to be designated for the purposes of the framework.

    b) **What are the likely consequences / implications of implementing this recommendation?**

Regulations specifying the name of a 'designated international agreement' under clause 3 could not commence until after the statutory disallowance period for those regulations under the *Legislation Act 2003* has expired. If this recommendation were adopted, this would mean that regulations would need to be amended to reflect any amendments to existing agreements, and those regulations could not commence until after the statutory disallowance period has expired.

4. **The Law Council recommends that proposed Schedule 1 to the TIA Act to "provide that, for an agreement with a foreign country or countries to be prescribed in regulations as a DIA, that agreement must be unclassified, in its entirety".**

    a) **What is the Department's response to this recommendation?**

All Australian treaties are unclassified in their entirety. In accordance with Australia's treaty-making requirements, treaties are tabled in Parliament to facilitate public consultation and parliamentary scrutiny. In addition, under Article 102 of the Charter of the United Nations, any treaty that comes into force must be registered with the United Nations and also published by it. Treaties are also published in the Australian Treaties Database.

    b) **What are the likely consequences / implications of implementing this recommendation?**

Not applicable as the treaty text will be entirely unclassified and subject to the parliamentary scrutiny process.

5. **The Law Council recommends that clause 182 of proposed Schedule 1 to the TIA Act be "removed to the extent it applies to regulations made under Clause 3 to list an agreement as a DIA, so that subsection 14(2) of the Legislation Act applies to agreements named in those regulations".**

    a) **What is the Department's response to this recommendation?**

Clause 182 provides that a reference to a designated international agreement in the regulations, an application, international production order or other instrument made under (proposed) Schedule 1 to the TIA Act, is a reference to that agreement as amended and in force for Australia from time to time. This provision is designed to remove any doubt about the validity of an international production order that has been issued or is in force at the time a new agreement is entered into. Further, this does not mean that amendments to agreements would not be subject to parliamentary and public scrutiny. As stated in the response to question 1 above, all amendments to designated international agreements will be subject to Australia's treaty-making requirements, including tabling in Parliament and consideration by the Joint Standing Committee on Treaties.

b) What are the likely consequences / implications of implementing this recommendation?

If the reference to agreements as 'amended and in force from time to time' in clause 182 were removed, this would mean an agreement would need to be specified as a new agreement in the regulations each time it is amended, extended or renewed for a further period.

This could lead to uncertainty about the status and/or operation of international production orders that have already been issued or are in force when a new agreement is entered into and comes into force. The risk of uncertainty could be greater if the recommendations referred to in questions 2 and 3 above were also to be adopted.

6. The Law Council recommends that clause 3 of proposed Schedule 1 to the TIA Act be amended "to provide that regulations prescribing an agreement as a DIA cannot be made unless the assurance obtained by the Minister for Home Affairs under Subclause 3(2) or 3(5) includes an assurance that Australian-sourced information will not be used by an authority of the foreign country in the prosecution of any offence for which the death penalty is a sentencing option".

a) What is the Department's response to this recommendation?

Clause 3 of the Bill is designed to be flexible as to the form, content and nature of the written assurance, as this depends on the particular foreign country's laws and practices in relation to the death penalty, and the scope of the particular agreement.

Currently, other international crime cooperation legislation and agreements do not completely exclude the ability for the Australian Government to share information or stipulate how that information may be used in death penalty cases. For example, under the *Mutual Assistance in Criminal Matters Act 1987*, Australia retains the discretion to decide whether to provide assistance in a death penalty case after considering the circumstances of the particular case. A written assurance allows for the risks associated with death penalty to be managed effectively while not prohibiting the sharing of information in all cases.

A foreign country's practices in relation to the death penalty, as well as the specific protections and safeguards in the agreement, will be subject to significant scrutiny at the agreement level.

b) What are the likely consequences / implications of implementing this recommendation?

This would represent a significant shift in Parliament's previous approach to international crime cooperation and death penalty matters. Inclusion of specific requirements in relation to written assurances would also bind Australia's negotiating position and could jeopardise Australia's ability to successfully finalise international agreements with foreign partner countries that have the death penalty, including the United States.

7. As an alternative to the recommendation referred to in the preceding question, the Law Council recommends that clause 3 of proposed Schedule 1 to the TIA Act be amended "to strengthen the conditions in subclauses 3(2) and 3(5) so that regulations prescribing an agreement as a DIA cannot be made unless the Minister for Home Affairs has obtained one of the following assurances from the foreign country or countries that are parties to the agreement:

- **Australian sourced information will not be used in death penalty cases; or**
- **Australian sourced information will be used, but the death penalty will not be sought or carried out; or**
- **Australian sourced information will be used only for exculpatory purposes."**

a) What is the Department's response to this recommendation?

Please see response to question 5.

b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 5.

8. The Law Council recommends that clause 3 of proposed Schedule 1 to the TIA Act be amended "to provide that the power to make regulations prescribing an agreement as a DIA must not be exercised unless the Attorney-General has issued a certificate attesting that he or she is reasonably satisfied of all of the matters listed in § 2523(b)(1)(B)(iii) of the US CLOUD Act, with respect to the foreign country's adherence to, and respect for, human rights. Regulations that do not comply with this requirement would be invalid".

a) What is the Department's response to this recommendation?

A foreign country's practices and adherence to human rights will be subject to significant scrutiny at the time an agreement is negotiated. As stated in the response to question 1 above, all designated international agreements will be subject to parliamentary and public scrutiny consistent with Australia's treaty-making requirements. In addition, any disallowable legislative instruments, including regulations specifying international agreements under clause 3 of the Bill, will be accompanied by a Statement of Compatibility with Human Rights and be scrutinised by the Parliamentary Joint Committee on Human Rights. Consistent with DFAT's treaty-making requirements, the Attorney-General is already required to approve the text of any Agreement before an Agreement can be signed.

b) What are the likely consequences / implications of implementing this recommendation?

Given that the Attorney-General is already required to approve the text of any agreement before an international treaty can be signed, and the involvement in the Attorney-General's Department in any development of a designated international agreement for the IPO Bill, it may be unnecessary to include a formal certification process for the Attorney-General.

It would also be open for the Joint Standing Committee on Treaties to consider a foreign country's adherence to, and respect for, human rights.

9. The Law Council recommends that clause 3 of proposed Schedule 1 to the TIA Act be amended "to include a specific condition on the power to make regulations listing an agreement as a DIA, to effectively limit the use by foreign countries of Australian-sourced information in their investigations and prosecutions of children. This should include an express condition to ensure that a foreign country will not use Australian-sourced information in the prosecution of children below the applicable age of criminal responsibility in Australia."

a) What is the Department's response to this recommendation?

Consistent with other international crime cooperation legislation, such as the *Mutual Assistance in Criminal Matters Act 1987*, specific human rights were not carved out of the ability to designate an international agreement under clause 3. Negotiations will ensure that human rights considerations and obligations are appropriately dealt with under each international agreement. A foreign country's practices and adherence to human rights, as well as the specific protections and safeguards in the agreement, will be subject to significant scrutiny at the agreement level.

b) What are the likely consequences / implications of implementing this recommendation?

Implementation would lead to inconsistency in how human rights is dealt with in international crime cooperation legislation.

10. The Law Council recommends that "Government should provide an unclassified explanation of the perceived need to include ASIO in the IPO scheme, including an explanation of the reasons that ASIO's existing foreign cooperation mechanisms are considered inadequate. The Explanatory Memorandum to the Bill should be amended to include that explanation. There should be an adequate opportunity for Parliamentary and public scrutiny of that explanation before the Bill is passed."

a) What is the Department's response to this recommendation?

On 14 May in public hearings to the Committee in reviewing this Bill, ASIO highlighted the importance the international production order framework will have in assisting ASIO in conducting its critical work in protecting Australia from threats to our security. This access will support the aim that Australian agencies, including our national security agencies, have continued, lawful access to the information they need to undertake their critical jobs to protect Australians and Australia from threats to our security.

ASIO's inclusion in the IPO regime provides a clear legislative pathway to ensure that ASIO is able to benefit from future international agreements for obtaining data directly from foreign communications providers. Many of the national security investigations undertaken by ASIO relate to the detection, prevention and investigation of serious crimes, including terrorism.

The Bill is not intended to replace existing foreign cooperation mechanisms but to complement current processes to ensure our agencies have every avenue available to them to protect public safety and combat serious crime. Existing mechanisms do not enable ASIO to compel production of data from foreign providers.

b) What are the likely consequences / implications of implementing this recommendation?

As highlighted by ASIO in its evidence given before the Committee, Australia faces unprecedented threats, including terrorism, espionage and foreign interference activities. The exclusion of ASIO from the IPO framework would result in ASIO being unable to access communications data and content relevant to security intelligence investigations to effectively counter these threats, especially given that many of these threats utilise communications and social media applications operated by United States owned companies. This would lead to increased risk to the Australian community from national security threats, including terrorism and espionage.

11. The Law Council recommends that proposed Schedule 1 to the TIA Act be amended "to define the terms 'criminal-law enforcement agency' and 'enforcement agency' for the purpose of the IPO scheme, by reference to the entities that are listed by name in existing ss 110A and 176A of the TIA Act."

a) What is the Department's response to this recommendation?

The Bill relies on the existing definitions of '*interception agency*', '*criminal-law enforcement agency*', and '*enforcement agency*' in the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to ensure that agencies have consistent access to both the domestic and international production order frameworks.

b) What are the likely consequences / implications of implementing this recommendation?

Implementing the recommendations as suggested would potentially create two separate lists of agencies for both the domestic and international production order frameworks. This may create confusion as to whether agencies can or cannot apply for certain types of powers. Consistency across both frameworks is critical to ensuring the agencies have similar access in terms of being able to obtain electronic evidence from domestic and international communications service providers.

12. The Law Council further recommends that the bill "provide that the Minister for Home Affairs may make a separate, disallowable legislative instrument under proposed Schedule 1 to the TIA Act declaring further

entities to be 'criminal-law enforcement' or 'enforcement' agencies for the purpose of the IPO scheme (in respect of some or all of their functions)."

a) What is the Department's response to this recommendation?

b) What are the likely consequences / implications of implementing this recommendation?

Implementation of this recommendation would require the Minister for Home Affairs to consider the appropriateness of the agency to access the international production order framework separately from consideration of the agency's access to the domestic framework. This would add an additional layer of administration and may lead to inconsistencies in agencies' ability to access the same type of information domestically and overseas.

13. The Law Council recommends that the provisions of the bill "authorising 'interception agencies' to apply for IPOs in subclauses 22(3), 33(3)(a), 52(3)(a) and 63(3)(a) of proposed Schedule 1 to the TIA Act should be amended to require agency heads to personally authorise any applicant for an IPO who is a 'member', 'staff member', 'official' whose position is not explicitly identified by reference to a designated level of seniority."

a) What is the Department's response to this recommendation?

The provisions for authorising applicants in law enforcement agencies in the Bill mirror the requirements under the TIA Act. This enables agencies to determine appropriate delegations based on their particular operational context and resourcing.

The Department notes that the provisions for authorising applicants in ASIO is partly different that the existing requirements under the TIA Act. This issue is also referred to in Appendix A on page 12.

b) What are the likely consequences / implications of implementing this recommendation?

The Bill recognises that each agency has separate requirements and accounts for this. For example, there would be inconsistency if a delegate for a domestic warrant did not also meet the applicable thresholds to be a delegate for the commensurate international production order.

14. The Law Council recommends that consideration "should also be given to amending subclauses 83(3) and 92(3) of proposed Schedule 1 to the TIA Act, to limit the Director-General of Security's power of authorisation to a defined class of ASIO employees by reference to seniority, such as 'senior position holders' as defined in section 4 of the ASIO Act."

a) What is the Department's response to this recommendation?

Please see Appendix A on pages 12 – 13, and note ASIO's separate response to a question taken on notice at the public hearing on 14 May 2020.

b) What are the likely consequences / implications of implementing this recommendation (i.e. if, more than just considering the proposed amendments, the proposed amendments were made)?

As above.

15. The Law Council recommends that clause 119 of proposed Schedule 1 to the TIA Act be amended "so that the Director-General of Security may only delegate their powers under Clause 116 to revoke national security IPOs to a Deputy Director-General and 'senior position holders' within the meaning of that term in section 4 of the ASIO Act, rather than any ASIO employee."

a) What are the likely consequences / implications of implementing this recommendation?

Please see Appendix A on page 12 - 13.

16. The Law Council recommends that the issuing of law enforcement and control order IPOs be restricted to "eligible judges" rather than members of the AAT.

a) What is the Department's response to this recommendation?

The utilisation of AAT members as independent decision-makers is appropriate, necessary and critical to the effective operation of the TIA Act and the Bill. AAT members currently play a critical role in authorising investigative powers under the TIA Act and have considered applications for interception warrants under the TIA Act since 1998. The role of nominated AAT members as independent issuing authorities also exists in other legislation such as the *Surveillance Devices Act 2004*.

The skill and experience of AAT members make them ideal candidates to assess applications for international production orders and make independent decisions on their compliance with the Bill. In addition, the framework and principles under which AAT members operate safeguards the functional independence of their decisions.

b) What are the likely consequences / implications of implementing this recommendation?

Implementing the recommendation would create inconsistencies with the domestic framework under the TIA Act. Law enforcement agencies have also advised that it would cause delays to investigations and prosecutions and impact operational outcomes if AAT members were not able to issue international production orders.

17. As an alternative to the recommendation referred to in the preceding question, the Law Council recommends that AAT members who can issue law enforcement orders "be restricted to Deputy Presidential and senior members, and members of the Security Division who have been admitted as Australian lawyers for a minimum of five years."

a) What is the Department's response to this recommendation?

Clauses 15–17 of the Bill restrict the AAT members that can be nominated or appointed to authorise IPOs to Deputy Presidents, senior members and members that are enrolled as a legal practitioner of a federal court or Supreme Court of a State or Territory and have been so enrolled for at least five years. This mirrors the existing provisions of the TIA Act.

Please see response to question 15.

b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 15.

18. The Law Council recommends that Parts 1 and 4 of proposed Schedule 1 be amended "to enable the Attorney-General to appoint judicial officers (comprising at least judges of the Federal Court of Australia) as issuing authorities for ASIO's national security IPOs, in addition to the power to appoint members of the Security Division of the AAT as issuing authorities."

a) What is the Department's response to this recommendation?

The Bill establishes nominated AAT Security Division members as independent decision-makers in recognition of the experience that AAT Security Division members have in relation to national security matters, which include matters that relate to ASIO such as the review of Qualified or Adverse Security Assessments issued under the ASIO Act. AAT Security Division members are considered appropriate due to their experience dealing with ASIO matters and the AAT Security Division's established security procedures, and infrastructure that enable the handling of ASIO's sensitive material.

Please see the response ASIO provided on this issue at the public hearing on 14 May 2020.

b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 17(a). Due to existing processes, the AAT has suitable infrastructure to deal with national security issues.

19. The Law Council recommends that clauses 89, 98 and 107 of proposed Schedule 1 to the TIA Act be amended "to require the issuing authority for ASIO's national security IPOs to consider the impacts of the proposed collection activity on the privacy of the target of the investigation, the B-Party (if applicable) and any other persons whose privacy may be impacted by the collection activity".

a) What is the Department's response to this recommendation?

Please refer to the response on this issue in the table at Appendix A responding to matters raised by IGIS (in particular the response to '*Statutory requirement to consider privacy and proportionality'* on page 10 of Appendix A). The Department also notes ASIO's advice to the Committee on the consideration of privacy impacts at the public hearing on 14 May 2020.

b) What are the likely consequences / implications of implementing this recommendation?

Please refer to the response on this issue in the above table responding to matters raised by IGIS (in particular the response to '*Statutory requirement to consider privacy and proportionality'* on page 9 of Appendix A).

20. The Law Council recommends that "passage of the IPO Bill should be contingent on the Government making a public commitment to introduce legislation, as soon as practicable and no later than within 12 months from the commencement of the IPO scheme, to amend the TIA Act and ASIO Act to align the thresholds and process for the issuing of ASIO's domestic telecommunications and special powers warrants with those applying to national security IPOs. In particular, ASIO's domestic warrants should be made subject to a two-staged authorisation equivalent to the requirements for its national security IPOs".

a) What is the Department's response to this recommendation?

On 30 May 2018, the Attorney-General announced that the Government had commissioned a Comprehensive Review of the legal framework governing the National Intelligence Community (also known as the 'Richardson Review'). As part of its terms of reference, the Richardson Review was required to examine the TIA Act. This Review handed its classified report to Government in December 2019. The Government is currently considering the findings of the Review.

b) What are the likely consequences / implications of implementing this recommendation?

This proposal concerns broader reforms to the TIA Act. As noted above, the Richardson Review's terms of reference required it to examine the TIA Act. The Government is currently considering the findings of the Review. As such, it would not be appropriate to pre-empt Government's consideration of the Review.

21. The Law Council argues that IPOs should not be available for the purpose of monitoring compliance with control orders and recommends that the bill be amended accordingly.

a) What is the Department's response to this recommendation?

The control order regime addresses the challenges posed by terrorism and involvement in hostile activity in a foreign country by mitigating the threat posed by individuals who have engaged in or have supported terrorism, or where a court otherwise considers a control order would substantially assist in preventing a terrorist act or support for, or facilitation of a terrorist act.

The use of domestic warrants and authorisations under the TIA Act to monitor those subject to control orders supports the monitoring of compliance with conditions imposed, and better mitigates the risk of terrorism and involvement in hostile activity in a foreign country. However, these powers are increasingly challenged by

Australians' increasing use of online communications platforms operated from foreign countries and data stored internationally, outside of Australian agencies' reach.

Accordingly, the Department considers it appropriate to enable the AFP to apply for control order international production orders to obtain information from designated communications providers based overseas that are covered by a designated international agreement. In some cases, suspected conduct may also constitute a serious criminal offence, such as preparations for a terrorist act, but the Department considers there should be no gap in law enforcement's ability to monitor individuals subject to Control Orders in relation to data that may be stored offshore.

Additionally, we note the AFP will only make applications for Control Orders to monitor people who present a significant terrorism risk to the community. Control order applications are considered by a court which, prior to issuing the Control Order, must be satisfied on the balance of probabilities that the order would substantially assist in protecting the public from a terrorist act, preventing the support of or facilitation of a terrorist act or engagement in hostile activities in a foreign country. Control Orders impose obligations, prohibitions and restrictions on a person.

In 2020, the AFP applied for and was granted control orders against convicted terrorist offenders upon release from prison after completing their head sentence. These orders have controls that limit their ability to use social media and communication based platforms. The use of social media platforms by a person on a Control Order constitutes a criminal offence that is punishable by a term of imprisonment. Timely access to evidence of these breaches through an IPO would be critical to the AFP's ability to respond rapidly, prosecute and enforce the breaches of control orders and ultimately assist in preventing an unacceptable escalation of risk to the Australian community. As such, IPOs for the purpose of monitoring and enforcing Control Orders would be an appropriate and proportionate law enforcement capability in the current threat environment.

It is well understood that terrorist threats can evolve rapidly, and the time between attack planning and execution can be very short. While the AFP can conduct monitoring warrants under section 3ZZOA of the *Crimes Act 1914* (Cth) and obtain Telecommunication Intercept and Surveillance Device warrants in relation to control order subjects, these have limitations.

- For example, if a control order subject was using an associate's device to access a social media account to contact prohibited associates.
- The ability to obtain an IPO in such circumstances would allow the AFP to access critical information stored offshore that may otherwise be unobtainable, at least in time to prevent possible imminent threat.

b) What are the likely consequences / implications of implementing this recommendation?

If a person subject to a control order perceives there is a low chance of non-compliance with the control order being detected, there is little incentive for them to comply with the terms of the order, and the specific preventative effect of a control order is potentially undermined. Control order international production orders ensure the Australian Federal Police have efficient access to critical information stored internationally to monitor compliance and mitigate risk of those subject to a control order.

22. The Law Council recommends that proposed Schedule 1 to the TIA Act be amended "to establish:

- **a panel of independent technical experts to support issuing authorities in considering all IPO applications; and**
- **a regime of 'special advocates' or 'public interest monitors' who can perform the role of contradictor in all IPO applications."**

a) What is the Department's response to this recommendation?

Both recommendations establish a different standard for determining applications for international production orders compared with authorisation of domestic warrants and authorisations under the TIA Act.
To this extent, these proposals relate to the broader operation of the TIA Act. The Richardson Review was required to examine the TIA Act as part of its terms of reference. The Government is currently considering the Review's findings.

There is currently no panel of independent technical experts or special advocates for existing TIA Act powers other than the Queensland and Victorian Public Interest Monitors (PIMs), and Public Interest Advocates for journalist information warrants. Independent decision-makers have not raised concerns with the current regime.

The role of the Victorian and Queensland PIMs has been included in the Bill as they play an analogous role in the application of domestic warrants. Should other jurisdictions legislate for a PIM, the TIA Act, including the international production order framework, may be amended to reflect the new offices. However, the establishment of a PIM is a matter for States and Territories to address.

b) What are the likely consequences / implications of implementing this recommendation?

Such a fundamental shift in legislating for a panel of independent technical experts, special advocates or PIM would require broader consideration in terms of reform to the TIA Act. The inclusion of such a panel in the international production order framework would deviate from the domestic regimes.

23. The Law Council recommends that the Government commit "to providing the necessary administrative support and resourcing to all IPO issuing authorities, including commitments with respect to:

- **providing regular briefings to all issuing authorities on the operational environment as relevant to IPO agencies;**
- **providing adequate resourcing for independent technical expertise and 'special advocates' or 'public interest monitors' to perform the role of contradictor in IPO applications; and**
- **amending the Explanatory Memorandum to identify the financial impacts of these measures. If there is a requirement under the Government's budget rules to offset any new funding allocated to these measures against existing expenditure, those offsets must not be drawn from the existing budgets of the federal courts, the AAT, oversight bodies or legal assistance programs."**

a) What is the Department's response to this recommendation?

The Department will prepare guidance for stakeholders on the operation of the legislation including issuing authorities.

Resourcing for the Queensland and Victorian PIMs is a matter for the Queensland and Victorian Governments.

b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 23.

24. The Law Council recommends that Part 7 of proposed Schedule 1 to the TIA Act be amended "to create an independent statutory review process for decisions to issue an IPO, including a process to resolve objections by the designated communications provider (DCP) and other persons that an IPO was not authorised by the relevant DIA, after it has been given to the DCP. That review process should involve the appointment of decision-makers who are independent to the ADA (for example, judicial officers appointed persona designata, or retired judicial officers). The decision-maker on review should be required to give reasons for their decision."

a) What is the Department's response to this recommendation?

The Bill provides for independent authorisation of international production orders. In addition, Australian courts will retain jurisdiction for judicial review of a decision 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 ensures that an affected person or a provider has an avenue to challenge decision-making.

The Australian Designated Authority will perform the role of ensuring that international production orders comply with the terms of the designated international agreements. The Australian Designated Authority will be the key facilitator and single point of contact for Australian agencies and foreign providers with experience, expertise and a broad view across international crime cooperation matters. The Bill contains a specific mechanism for designated communications providers to raise objections with the Australian Designated Authority, and it is anticipated the international agreements themselves will also contain processes for objections and resolution of disputes between governments and between providers and governments. Decisions of the Australian Designated Authority will also be subject to judicial review.

b) What are the likely consequences / implications of implementing this recommendation?

This would unnecessarily duplicate the role of the Australian Designated Authority and create inefficiencies.

25. The Law Council recommends that clause 122 of proposed Schedule 1 to the TIA Act be amended "to require the ADA to cancel an IPO it has given to a DCP, if it considers that the IPO is not consistent with the terms of the underlying DIA."

a) What is the Department's response to this recommendation?

Clause 122 of the Bill stipulates the Australian Designated Authority may cancel an international production order. The construction gives adequate flexibility for agreed review and dispute resolution processes to operate by virtue of designated international agreements. For example, a designated international agreement may allow a designated communications provider to raise an objection to the requesting party's authorities on particular grounds and set out a process for that to occur.

Administrative guidance will also set out the procedures and process that the Australian Designated Authority will go through when it receives an objection from a designated communications provider.

If an order is found to be incompatible with the agreement after an objection has been raised by a designated communications provider (in circumstances there was an original assessment that it was compliant), the Australian Designated Authority would be under an obligation under the designated international agreement to ensure that the order is not progressed.

b) What are the likely consequences / implications of implementing this recommendation?

Adopting this recommendation would limit Australia's flexibility – under the proposed model the ultimate outcome if there is non-compliance with the international agreement is the international production order would be cancelled. However, the construction adopted in the Bill provides an ability to remedy issues before this is to occur.

26. The Law Council recommends that the "Government (or either House of Parliament, by resolution) should refer to the PJCIS the matter of whether the exemption of aggregated statistical information from ASIO's unclassified annual reports (including the proposed exemption of statistical information relating to IPOs) is necessary and appropriate in contemporary circumstances. In conducting this review, the PJCIS may request the INSLM to consider the matter and report back to the PJCIS."

a) What is the Department's response to this recommendation?

As noted in Appendix A on page 15, ASIO is not currently required to include statistical reporting on its use of the TIA Act in its public annual report.

b) What are the likely consequences / implications of implementing this recommendation?

The inclusion of statistics in an unclassified annual report would highlight specifically how much ASIO utilises the international production order framework. This may permit inferences to be drawn as to how ASIO utilises the proposed international production order framework, and may assist persons of interest to change their behaviour due to public reporting on the use of investigatory powers.

27. The Law Council recommends that Parts 2, 3 and 4 of proposed Schedule 1 to the TIA Act be amended "to ensure that the obligations on law enforcement agencies to notify the Ombudsman of certain matters, and the obligations on ASIO to inform the IGIS of certain matters, are consistent with each other, by adopting the higher of the two standards where there is a difference".

a) What is the Department's response to this recommendation?

In its submission to the Committee, the Law Council of Australia made two suggestions for implementation of this recommendation:

- ASIO should be required to notify IGIS as soon as practicable if it breaches its obligation in clause 116 to revoke an international production order if satisfied that the issuing grounds have ceased to exist (to be consistent with the obligation on law enforcement agencies with respect to control order international production orders); and
- If the Attorney-General gives oral consent to a law enforcement agency to make an application for an international production order under Part 2 or 3, the agency must give the Ombudsman a copy of a written record of that consent within 3 working days (to be consistent with the obligation on ASIO to provide that record to IGIS) (pages 42–43 of the submission).

In relation to the first sub-point, the notification requirements in the Bill in relation to this issue mirror the existing requirements in the TIA Act. To the extent that this proposal would establish a different requirement, it relates to the broader operation of the TIA Act. The Richardson Review was required to examine the TIA Act as part of its terms of reference. The Government is currently considering the Review's findings`. The IGIS will provide oversight over ASIO's compliance with the requirements in relation to revocation of orders.

In relation to the second sub-point, there is no notification requirement for law enforcement agencies as the Attorney-General does not play any role in consenting to applications for international production orders under Part 2 or 3 of the Bill.

b) What are the likely consequences / implications of implementing this recommendation?

Please refer to the response above.

28. The Law Council recommends that subclauses 153(1)(p) and (q) of proposed Schedule 1 to the TIA Act be amended "to:

- **omit the references to the Inspector-General of Intelligence and Security Act 1986 (Cth) and the Ombudsman Act 1976 (Cth); and**
- **provide that IGIS and Ombudsman officials do not bear the evidential burden for these exceptions, in relation to their status as IGIS or Ombudsman officials, and the fact that they dealt with the relevant information in their official capacities."**

a) What is the Department's response to this recommendation?

In relation to the first sub-point, please refer to the response in Appendix A at page 17.

In relation to the second sub-point, the Bill does not include this provision as it has been modelled as closely as possible on the domestic warrant framework in the TIA Act

b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 28(a).

29. The Law Council recommends that the IGIS Act be amended "to enable IGIS officials to give protected IPO information to the Ombudsman and ADA, in relation to the oversight of ASIO's national security IPOs. The purposes of the permitted disclosures should be to:

- **respond to a request for assistance from the Ombudsman in relation to the Ombudsman's oversight of the ADA's administration of ASIO's national security IPOs; and**
- **discuss with the ADA matters relating to ASIO's national security IPOs that are relevant to the functions of both IGIS and the ADA, including the compliance of those IPOs with the underlying DIAs."**

a) What is the Department's response to this recommendation?

Please see Appendix A on page 17.

b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 29(a).

30. The Law Council recommends that the INSLM Act be amended "to ensure that the INSLM has full oversight of the legislation establishing the IPO scheme. This should include as part of the INSLM's annual reporting function, and a one-off statutory review after the legislation has been in force for a set period of time, between 12-18 months of operation."

a) What is the Department's response to this recommendation?

The Independent National Security Legislation Monitor has an existing power under section 6 of the *Independent National Security Legislation Monitor Act 2010* to self-initiate a review of the operation, effectiveness ad implications of any Commonwealth Law to the extent that it relates to Australia's counter-terrorism and national security legislation. This would enable the INSLM to conduct a review of the operation of the IPO framework on his or her own motion.

If the INSLM were to conduct such a review, it would be more appropriate for the review to occur a considerable time after passage of the legislation. For example it is unlikely that orders under the first bilateral agreement will be sent under the legislation for between 8-12 months given domestic treaty processes that need to be observed. Any review should be done a significant period after the designation of an agreement under the legislation. This would ensure that implementation measures for both the IPO framework and international agreement, including procedures, training and technical systems, are well established and have been utilised by agencies for a sufficient period prior to the review taking place.

b) What are the likely consequences / implications of implementing this recommendation?

Please see the response to question 30(a).

31. Law Council recommends that Part 4 of the Intelligence Services Act 2001 be amended to:

- **"enable the PJCIS to undertake ongoing monitoring of all of the activities of ASIO and the AFP under the IPO scheme, including consideration of relevant provisions of the AFP and ASIO's annual reports on IPOs;**

- **require the PJCIS to conduct a review of the operation of the IPO scheme after a set period of operation, in the range of 12-18 months;**
- **enable the PJCIS to require the ADA to provide it with briefings on request."**

a) What is the Department's response to this recommendation?

Agencies' use of the international production order framework and the Australian Designated Authority will be subject to comprehensive operational oversight by the Commonwealth Ombudsman and IGIS.

The Department notes that the Committee has existing functions under section 29 of the *Intelligence Services Act 2001* to review the administration and expenditure of ASIO and matters relating to ASIO that have been referred to the Committee, and to monitor and review legislation referred to it.

Currently the Australian Designated Authority is not required to provide briefings on request to the PJCIS. Pursuant to section 30 of the *Intelligence Services Act 2001*, it would be open for the PJCIS to request briefings from the Commissioner of the AFP or Director-General of Security on the AFP and ASIO's use of the international production order framework to support their functions in relation to the Australian Intelligence community.

In the event that the Committee were to conduct a statutory review relating to the IPO framework within a set period of time, it would be more appropriate for the review to occur a significant period after the operationalisation of the first designated international agreement. This would ensure that implementation measures for both the IPO framework and international agreement, including procedures, training and technical systems, are well established and have been utilised by agencies for a sufficient period prior to the review taking place.

b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 31(a).

32. The Law Council recommends that proposed Schedule 1 of the TIA Act be amended "to establish the Australian Designated Authority as an independent statutory office holder."

a) What is the Department's response to this recommendation?

The establishment of a Designated Authority for Australia is a requirement under the proposed CLOUD Act agreement with the United States. The Australian Designated Authority will act as a central authority for the implementation of all designated international agreements under the Bill.

The Secretary of AGD (supported by AGD) is an appropriate officer to perform the functions of the Australian Designated Authority. As Australia's international crime cooperation central authority, AGD is best placed to leverage existing international crime cooperation relationships and monitor the interactions between the international production order and mutual legal assistance frameworks.

The Bill also provides comprehensive oversight and record keeping that lends to transparency in the operation of the international production order framework. This includes public reporting by law enforcement agencies and the Australian Designated Authority, and ministerial reporting to the Australian Parliament similar to the annual reporting requirements for the existing regimes under the TIA Act.

b) What are the likely consequences / implications of implementing this recommendation?

The proposal would complicate existing approaches that work well in current international legal cooperation processes.

33. The Law Council recommends that clause 179 of proposed Schedule 1 to the TIA Act be amended "to provide that the Australian Designated Authority may only delegate their functions and powers to an

employee who is admitted as an Australian legal practitioner, and is in a position classified as Senior Executive Service Band 1 or higher."

a) What is the Department's response to this recommendation?

Given the broad range of functions that will be performed by the Australian Designated Authority, it is appropriate that the Secretary of AGD is able to determine appropriate delegations.

The Bill permits the Secretary of AGD, as the Australian Designated Authority, to delegate his or her powers and functions to a senior executive or executive-level employee within AGD. The delegation may be subject to directions. The ability to delegate to an appropriately senior employee is important to streamline the day-to-day operations of the Australian Designated Authority. This approach is consistent with the approach taken in international crime cooperation more broadly.

b) What are the likely consequences / implications of implementing this recommendation?

Implementing this recommendation could have resourcing and efficiency implications for the Attorney-General's Department.

34. The Law Council recommends that clause 140 of proposed Schedule 1 to the TIA Act be amended "to require agencies to undertake periodic reviews of information obtained under interception and stored communications IPOs to assess whether the obligation to destroy irrelevant information under Clause 140 is enlivened."

a) What is the Department's response to this recommendation?

Please see Appendix A on page 15.

b) What are the likely consequences / implications of implementing this recommendation?

Please see Appendix A on page 15.

35. The Law Council argues that "[i]n the absence of compelling evidence to support a claim that it would be impracticable to do so, the obligations imposed on agency heads under Clause 140 of proposed Schedule 1 to delete irrelevant information from their holdings should be amended to apply to telecommunications data obtained under an IPO."

a) What is the Department's response to this recommendation?

Please see response to question Appendix A on page 15.

b) What are the likely consequences / implications of implementing this recommendation?

Please see Appendix A on page 15.

36. The Law Council recommends that "[t]he Government should, as a matter of priority, develop administrative guidance on the application of the IPO scheme and release these materials publicly for consultations before they are finalised and published, prior to the commencement of the amendments. This should include completion of a review of the Minister's Guidelines to ASIO, and the issuing of new guidelines under section 8A of the ASIO Act, as a matter of urgency."

a) What is the Department's response to this recommendation?

The Department will prepare guidance for stakeholders on the operation of the legislation and the CLOUD Act agreement once finalised. This will include guidance for agencies, the Australian Designated Authority and industry. Stakeholders will be consulted on the development of these materials prior to their finalisation.

Matters relating the ASIO Guidelines are dealt with above.

b) What are the likely consequences / implications of implementing this recommendation?

Please see response to question 23(a).

37. The Law Council recommends that subclause 161(3) of proposed Schedule 1 to the TIA Act be amended "to provide that evidentiary certificates able to be issued by a DCP in relation to acts and things done to comply with an IPOs are of a prima facie nature."

a) What is the Department's response to this recommendation?

Subclause 161(3) of the Bill is consistent with the approach taken for provider evidentiary certificates in the TIA Act. These provisions specify that certificates are conclusive evidence of the matters stated in the certificate where they cover technical matters that are sufficiently removed from the main facts at issue. This will ensure that Australian courts have complete information before them to assist in the administration of justice.

This provision recognises the difficulties associated with having staff from communications providers attend court to give witness testimony on technical or formal matters undertaken by the provider to comply with an order. These difficulties are expected to be greater under the international production order framework as designated communications providers will be based overseas and would need to travel internationally to attend court in Australia. In addition, it is expected that large global communications providers may receive a high number of international production orders.

This provision does not prevent a defendant from challenging the admissibility of illegally or improperly obtained evidence during proceedings. The presiding judge retains discretion over whether to admit evidence.

b) What are the likely consequences / implications of implementing this recommendation?

Implementation of the recommendation would make the Bill inconsistent with the domestic warrant framework. It would also likely result in difficulties arising at trial where an employee of the foreign provider who complied with an order, would have to attend court to be questioned on technical matters not related to facts in dispute or matters that go to questions of legality. This could jeopardise the usefulness of the international production order framework.

38. The Law Council recommends that clause 126 of proposed Schedule 1 to the TIA Act "be amended to provide that the Secretary of the Attorney-General's Department, and not the Communications Access Co-Ordinator, is the 'authorised applicant' for the purpose of the enforcement provisions in Part 8."

a) What is the Department's response to this recommendation?

The Communications Access Co-ordinator (CAC) is an existing statutory role under s6R of the TIA Act, which is performed within the Department. The CAC is the primary point of liaison for interception agencies, telecommunications carriers and carriage service providers in relation to telecommunications interception and data retention issues. Amongst other things, the CAC performs a coordination role and liaises with the telecommunication industry on behalf of interception agencies.

The CAC's role as the authorised applicant in relation to a civil penalty provision under Part 8 of (proposed) Schedule 1 to the TIA Act is consistent with the CAC's existing role as the authorised applicant for enforcement of industry assistance notices under Part 15 of the *Telecommunications Act 1997* (as amended by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Assistance and Access Act)).

b) What are the likely consequences / implications of implementing this recommendation?

This would lead to would lead to inefficiencies and duplication as the CAC has existing functions in relation to enforcement under a related Act.

39. Could the Department please outline – in detail – how client legal privilege is protected under the proposed IPO scheme?

Subject to the legislative thresholds and requirements, the powers under the international production order scheme authorise access to certain communications, regardless of whether the communication might be the subject of LPP. Moreover, when complying with an international production order, communications providers are not required to analyse and withhold material on the basis that such material could potentially be subject to a claim of LPP.

Communication obtained under the international production order scheme that may be subject to LPP will be dealt with in accordance with the laws of evidence, generally at the point in time that LPP is claimed. This is consistent with how such material obtained under the TIA Act is dealt with.

The IPO Bill is consistent with other forms of international crime cooperation mechanisms such as mutual legal assistance. Information may be obtained that could potentially contain LPP information. Similar to information obtained domestically, it would also be dealt with in terms of laws of evidence.

As a matter of practice, the Department understands that agencies have internal processes and generally adopt a cautious approach and quarantine any material received under a TIA Act authorisation or warrant that could potentially be subject to a claim of LPP.

40. The Allens Hub recommends that the IPO Bill be "consistent with the government's scheme for protecting COVIDSafe app data from access by domestic and international national security and law enforcement agencies".

a) What is the Department's response to this recommendation?

It is an offence under the *Privacy Amendment (Public Health Contact Information) Act 2020* (COVIDSafe legislation) to disclose data collected by the COVIDSafe app to any person outside Australia. This offence applies to service providers who host that data and attracts a penalty of five years' imprisonment and/or 300 penalty units. While the IPO Bill does permit Australian agencies to request the disclosure of data from foreign providers and vice versa, it does not create any exemptions to, or override, the prohibitions in the COVIDSafe legislation.

The Department also notes that international agreements under the IPO framework would likely include further complementary safeguards to protect sensitive Australian data from foreign government incoming requests.

b) What are the likely consequences / implications of implementing this recommendation?

Please refer to the answer to question 40(a).

41. The Allens Hub recommends that there be "consistent protections for telecommunications data held domestically and data held offshore by making the domestic access regime consistent with the higher standards for an outgoing international production order".

a) What is the Department's response to this recommendation?

Please see A at page 11, and question 39 above.

b) What are the likely consequences / implications of implementing this recommendation?

Please see Appendix A at page 11, and question 39 above.

42. *For the Department of Home Affairs:* Please provide a breakdown of how many times a year each law enforcement and security agency in Australia makes use of the existing mutual assistance framework to access information held in the United States.

The Department does not hold these statistics. The Attorney-General's Department is the central authority for the purposes of mutual assistance requests under the *Mutual Assistance in Criminal Matters Act 1987*. The

Department contacted the Attorney-General's Department who provided the following response to this question.

The International Crime Cooperation Central Authority (ICCCA) in the Attorney-General's Department has sent the following number of mutual assistance requests (MARs) to the United States of America in each year between 2014 and 2019 at the request of the agencies listed below. No national security agency requested ICCCA make a MAR to the US.

CAVEAT: Due to limitations with the reporting functionality of ICCCA's database, the below statistics have been extracted by an examination of over 800 individual MAR files. Every effort has been made to ensure, in the time provided by the Committee, they are as accurate as possible.

At the request of the Australian Federal Police (AFP), Australia made the following number of MARs to the US:

- In 2014 - 13
- In 2015 - 15
- In 2016 - 19
- In 2017 - 14
- In 2018 - 21
- In 2019 - 20

Note: Eight of these MARS were made at the request of ACT Policing, which is an arm of the AFP.

At the request of the Commonwealth Director of Public Prosecutions (CDPP), Australia made the following MARs to the US:

- In 2014 - 21
- In 2015 - 15
- In 2016 - 15
- In 2017 - 12
- In 2018 - 9
- In 2019 - 9

Note: The MARs listed in paragraph 2 are different to the MARs listed in paragraph 1. In many instances the MARs listed in paragraph 2 were requested by the CDPP to support the prosecution of matters that were investigated by the AFP. The AFP often had an active involvement in the progress of the MARs listed in paragraph 2.

At the request of the New South Wales Police Force, Australia made the following number of MARs to the US:

- In 2014 - 17
- In 2015 - 19
- In 2016 - 12
- In 2017 - 15
- In 2018 - 23
- In 2019 - 27

At the request of the Queensland Police Service, Australia made the following number of MARs to the US:

- In 2014 - 15
- In 2015 - 16
- In 2016 - 13
- In 2017 - 8
- In 2018 - 12
- In 2019 - 8

At the request of South Australia Police, Australia made the following number of MARs to the US:

- In 2014 - 7
- In 2015 - 4
- In 2016 - 2
- In 2017 - 1
- In 2018 - 4
- In 2019 - 4

At the request of Tasmania Police, Australia made the following number of MARs to the US:

- In 2014 - 0
- In 2015 - 0
- In 2016 - 0
- In 2017 - 0
- In 2018 - 1
- In 2019 - 1

At the request of Victoria Police, Australia made the following number of MARs to the US:

- In 2014 - 2
- In 2015 - 6
- In 2016 - 9
- In 2017 - 8
- In 2018 - 7
- In 2019 - 5

At the request of Western Australia Police, Australia made the following number of MARs to the US:

- In 2014 - 1
- In 2015 - 0
- In 2016 - 1
- In 2017 - 4
- In 2018 - 1
- In 2019 – 1

At the request of Northern Territory Police, Australia made the following number of MARs to the US:

- In 2014 - 0
- In 2015 - 0
- In 2016 - 0
- In 2017 - 1
- In 2018 - 0
- In 2019 – 1

43. *For the Department of Home Affairs:* In total, how many IPO requests does the Department estimate that Australian law enforcement and security agencies will make each year if this bill becomes law and Australia and the United States become parties to a designated international agreement?

Please refer to the response the Department provided on this issue at the public hearing on 14 May 2020.