Law Council
OF AUSTRALIA

Review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)

Supplementary Submission

Parliamentary Joint Committee on Intelligence and Security

10 August 2020

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2020 Executive as at 1 January 2020 are:

- Ms Pauline Wright, President
- Dr Jacoba Brasch QC, President-elect
- Mr Tass Liveris, Treasurer
- Mr Ross Drinnan, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council gratefully acknowledges the assistance of its Privacy Law Committee of the Business Law Section in the preparation of this supplementary submission.

Introduction

1. The Law Council is pleased to provide this supplementary submission to the inquiry of the Parliamentary Joint Committee on Intelligence and Security (**Committee**) into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA Act**).

2. This submission supplements the Law Council's evidence to the Committee at its public hearing on 27 July 2020. Committee members expressed interest in receiving a further written submission from the Law Council detailing its views on the recommendations of the third Independent National Security Legislation Monitor (**INSLM**), Dr James Renwick CSC SC, in his report of 30 June 2020, entitled *Trust But Verify: A Report Concerning the Telecommunications And other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters* (**INSLM report**).[1]

3. The Law Council has provided its comments on each of the INSLM's 33 recommendations in **Appendix 1**. This appendix also highlights several outstanding issues that were not the subject of examination in the INSLM report, in respect of which the Law Council continues to recommend amendments.[2]

4. The Law Council's specific comments in Appendix 1 on individual INSLM recommendations and other outstanding issues should be read with the more general commentary in the main body of this submission. This commentary:

   - outlines the Law Council's overall position on the INSLM report, and the key findings on matters of principle which underpin the INSLM's recommendations;
   - highlights selected key issues that were the focus of questioning at the public hearing. These issues arise from INSLM recommendations 3-6 (independent issuing body for industry assistance notices) and 12 (removal of AFP approval functions for State and Territory police industry assistance notices); and
   - provides further information to the Committee about a recent decision of the Court of Justice of the European Union (**CJEU)** known as 'Schrems II', which may have broader relevance to the interaction of the TOLA Act measures with the European Union General Data Protection Regulation (**GDPR**).

5. In addition, the Law Council notes that the Government released the *2020 Cybersecurity Strategy* on 6 August 2020. This strategy foreshadows an intention to bring forward various legislative proposals. These include the conferral of an 'offensive' power on the Australian Federal Police and Australian Criminal Intelligence Commission that would enable these agencies to enlist the technical assistance of the Australian Signals Directorate to disrupt serious criminal activities on the 'dark

[1] Independent National Security Legislation Monitor, *Trust But Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, (30 June 2020) (INSLM Report).

[2] Key issues raised by the Law Council and other stakeholders are summarised in: Parliamentary Joint Committee on Intelligence and Security, *Report on the Review of the TOLA Act* (April 2019), 9-119 (Appendix A: summary of evidence).

web'.[3] It has been reported that the Government intends to introduce and seek passage of legislation within the 2020 sitting year.[4]

6. In addition to such a major expansion of powers requiring thorough scrutiny in its own right (which should include the release of an exposure draft before a Bill is introduced) this proposal would appear to raise issues of interaction with the TOLA measures in Schedule 2 (computer access warrants) and potentially Schedule 1 (industry assistance).

7. Given the potential for extensive interaction, the Law Council considers it is important that there is thorough consultation and scrutiny on the further proposals. This would preferably be done via the public release of an exposure draft, with an appropriate consultation period, in advance of more complex and voluminous legislation being introduced to Parliament, especially if there is an intention to seek passage in 2020.

Law Council position on the INSLM report

Overall position on INSLM recommendations

8. As indicated at the Committee's public hearing of 27 July 2020, the Law Council supports the former INSLM's recommendations, eighteen of which endorse, in full or in principle, the submissions of the Law Council.[5]

9. The Law Council urges the Committee to support the implementation of the INSLM's recommendations. Although some of the INSLM's recommendations have adopted the Law Council's submissions for alternative amendments rather than its preferred options,[6] they would nonetheless make substantial improvements to the legislation.

INSLM conclusions on necessity and proportionality

10. The Law Council supports the conclusions of the INSLM, documented at pages 24-25 of the INSLM Report, that the TOLA Act measures:

    - **are necessary**, or are likely to be necessary, to enable security and law enforcement agencies to overcome the challenges presented by the ubiquitous use of encryption, subject to two exceptions that require amendments to Schedules 1[7] and 5;[8] but

    - **are not proportionate** to the security and law enforcement objectives to which they are directed. However, they could be made proportionate if the INSLM's recommended amendments are implemented. (The Law Council

[3] Australian Government, *2020 Cybersecurity Strategy*, 6 August 2020, [6]. See also: the Hon Scott Morrison MP, Prime Minister of Australia, and the Hon Peter Dutton MP, Minister for Home Affairs, *Transcript of Press Conference: Australian Parliament House, Thursday 6 August 2020*, Media release, 6 August 2020, 8.

[4] Michelle Grattan, 'Morrison pursues tougher powers in fight against cyber attacks and criminals' activity', *The Conversation*, 10 August 2020, <https://theconversation.com/morrison-pursues-tougher-powers-in-fight-against-cyber-attacks-and-criminals-activity-144027>.

[5] Parliamentary Joint Committee on Intelligence and Security, *Report on the Review of the TOLA Act* (April 2019), recommendations 3-10, 29, 14-15, 17, 19-20, 22, 23 and 33, and the conclusion at [12.5].

[6] Ibid, recommendations 8-10 (definition of 'systemic weakness' and component terms).

[7] Ibid, see recommendation 1: extension of the industry assistance scheme, as amended in line with the INSLM's recommendations, to State and Territory anti-corruption agencies.

[8] Ibid, see recommendations 19-22: scope of, and authorisation requirements applying to, ASIO's power to confer civil immunities on persons whose assistance it requests to perform its functions under subsection 21A(1) of the *Australian Security Intelligence Organisation Act 1979* (Cth).

considers that the requirements of proportionality also necessitate implementation of the outstanding issues detailed in Appendix 1 that were not addressed in the INSLM report, and remain of concern.)

Matters of principle in relation to proportionality

11. On the general issue of proportionality, the Law Council agrees with the key findings of the INSLM on the matters of principle set out Chapters 7-10 of his report. These principles underpin his findings on the proportionality of individual measures, and his recommendations to address those measures found to be disproportionate.

12. In particular, the Law Council concurs with the following key propositions in the report:

'Trust but verify'

13. The overarching principle in the INSLM's report, as reflected in its title, is that the existence of independent, retrospective oversight of agencies' intrusive investigative activities is not sufficient to secure public trust and confidence.

14. Rather, the INSLM considered that clear statutory safeguards are necessary to provide legal limitations on the scope of those powers, rather than making their exercise heavily dependent on wide executive discretion by agencies or their Ministers. The INSLM also considered it essential that an independent body is responsible for authorising compulsory industry assistance powers, not the agencies themselves or ministers such as the Attorney-General.[9]

The need for even stronger safeguards in the digital world than the physical world

15. The INSLM considered that there is a greater need for safeguards of the kind described above in the digital world, given the wide and potentially unknown or unascertainable impacts of technology. The INSLM also emphasised the importance of an independent issuing body having access to independent technical advice, to ensure that they understand the privacy and other implications of intrusive digital surveillance and related powers.[10]

The false distinction between access to content, and enabling access

16. The INSLM rejected a purported distinction between the power of a law enforcement agency or the Australian Security Intelligence Organisation (**ASIO**) to access the content of digital communications, and the powers of those agencies to require a communications provider to render technical assistance to give them the ability to access such content. The INSLM considered that this distinction improperly elevated substance over form. This view was a key basis for his recommendations for the independent authorisation for technical assistance notices (**TANs**) and technical capability notices (**TCNs**).[11]

[9] Ibid, 23, 34-35, 185-187, 195-196 and 201-202.

[10] Ibid, 141-142 and 193-194.

[11] Ibid, 193-194.

Recommendations 3-6 – independent issuing of industry assistance notices

17. The INSLM recommended that TANs and TCNs should be issued by an independent body – namely, a new Investigatory Powers Division of the Administrative Appeals Tribunal (**AAT**) which is presided over by a retired judge, who is appointed to the new office of the Investigatory Powers Commissioner (**IPC**).

The need for independent issuing of TANs and TCNs

18. As noted in the Law Council's evidence to the Committee on 27 July 2020, the Law Council strongly supports the principle that TANs and TCNs should be issued independently to security and law enforcement agencies and Ministers.

19. This reflects the longstanding position of the Law Council that all intrusive investigatory powers should be authorised by an independent authority who has appropriate adjudicative expertise, experience and eminence, and is given all necessary access to independent technical expertise.

The nature of the issuing function and status of the issuing body

20. The Law Council acknowledges that the INSLM identified several benefits in establishing a permanent body to issue compulsory industry assistance notices. One of the most significant anticipated benefits is the development of deep institutional expertise in applicable laws and technologies.[12]

21. However, the Law Council recommends that further consideration is given to conferring the authorisation power on a court, as a judicial function, in preference to conferring the function on an administrative tribunal that is part of the executive arm of government. The Law Council considers that the interests of independence – both substantive and perceived – tend strongly in favour of a judicial issuing function.

22. This is particularly because a judicial officer (whether they are exercising judicial power as a member of a court, or are exercising an executive power conferred *persona designata*) is constitutionally bound to act judicially. That is, they must perform the relevant function 'in a just and fair manner, with judicial detachment'[13] and bring to bear the 'skill and experience judicial officers'.[14]

23. As the INSLM identified, the conferral of a judicial authorisation function on a court would require the resolution of certain constitutional and other procedural issues. However, as the INSLM also acknowledged, those issues are not insurmountable.[15]

24. The establishment of an independent body would be a landmark structural reform to the authorisation framework for security agencies' coercive and intrusive powers. While the transition to any model of independent authorisation would be an improvement on the current authorisation arrangements for the industry assistance scheme, the Law Council submits that further investigation of the available options for the nature and composition of that body is necessary.

---

[12] INSLM Report, 219.

[13] *Love v Attorney-General (NSW)* (1990) 169 CLR 307 at [28] (Mason CJ, Brennan, Dawson, Toohey and Gummow JJ).

[14] *Hilton v Wells* (1985) 157 CLR 57 at [13] (Mason and Deane JJ).

[15] INSLM Report, 216-218.

‘Future proofing’ an independent issuing body

25. The Law Council also encourages the Committee, in considering the potential establishment and composition of an independent issuing body, to take a broad and longer-term view of its prospective functions. For example, the independent authority could have the power to issue International Production Orders,[16] and potentially some or all federal intelligence and law enforcement evidence collection warrants.

26. The specific details of any broader functions would properly be considered in the future – potentially in the context of considering the presently unreleased reports of the Comprehensive Review of Intelligence Legislation, completed by Mr Dennis Richardson AO in 2018-19. However, it would be highly desirable for a new body to be designed in a way that would make it feasible for its authorisation functions to be expanded in the future, so that this option would be available as required.

Critical safeguards if an administrative tribunal is preferred over a court

Statutory process and eligibility requirements for appointment

27. If the Committee is minded to support the establishment of an Investigatory Powers Division of the AAT, in preference to the conferral of judicial issuing functions, it will be crucial that the statutory powers of appointment and termination of office are robust and do not leave open the potential for any actual or perceived bias or conflicts of interest to arise.

28. In addition to recommendations of the INSLM with respect to the qualifications and appointment of the Investigatory Powers Commissioner,[17] it will also be critical that there is an open, transparent and consultative process for appointing the Commissioner and members of the new division. The independence and integrity of the new division will depend on there being an apolitical, open, transparent and merit-based appointment system. This should include community consultation, including consultations with the legal profession, to safeguard the quality and diversity of appointments.

29. The Law Council considers it essential that there are statutory appointment criteria prescribing the requisite fields and levels of expertise of all members. Given the connection between compulsory industry assistance notices with criminal investigations and warrant-based collection powers, the eligibility criteria should include a requirement that legally qualified members must have considerable experience and expertise in criminal law (especially in the conduct of criminal trials) as senior legal practitioners (for example, as senior counsel or a managing partner of a law firm specialising in criminal law). The assessment of a candidate’s expertise must not be left to the sole or substantial discretion of Ministers without clear and precise statutory direction about the subject-matter and quantum of that expertise.

30. There should also be robust disqualification and mandatory termination criteria to avoid all instances of actual, potential and perceived conflicts of interest. This must include criteria that cover all conflicts of interests arising from a person’s past and

[16] Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020 (Cth).

[17] INSLM Report, recommendation 6 (appointment of the Commissioner by the Governor-General on the advice of the Attorney-General, following consultation with the Opposition; and an eligibility criterion that the person is a retired judge of the Federal Court or a Supreme Court of a State or Territory).

present employment, and in the case of any part-time appointees, their future employment, if it is known at the time of their proposed appointment.[18]

Consultation on draft legislation

31. The matters outlined above are integral to the effectiveness of, and public confidence in, such a tribunal, should the Committee support the INSLM's recommendations for its establishment and composition. Consequently, meaningful consultation on exposure draft legislation would be essential, in addition to detailed Parliamentary scrutiny of a Bill once it is introduced. The Law Council, as the national body for the legal profession, should be included in such consultations before a Bill is introduced to Parliament.

Form of amending legislation

32. It is also important that any amending legislation to establish an independent issuing body is not contained in an 'omnibus Bill' in the nature of the TOLA Act. The latter Act conferred or extended multiple, discrete intrusive powers in five voluminous and complex schedules, which the Parliament was requested to scrutinise and pass in a highly compressed timeframe.

33. Such an approach to the design of amending Bills is not conducive to effective parliamentary or public scrutiny of the proposed amendments. This is particularly problematic in the case of proposals to confer or expand highly intrusive and coercive investigatory powers, such as those in the TOLA Act. Regrettably, this was evident in the relatively limited capacity of the INSLM, the Committee and inquiry participants to engage in detail with Schedules 2-5 of the TOLA Act in addition to the industry assistance scheme in Schedule 1.

34. The Law Council considers that the above legislative design practices adopted in relation to the TOLA amendments have proven detrimental to the quality of the legislation and is concerned to ensure that this practice is not repeated, condoned or normalised. This approach to the introduction and enactment of legislation within timeframes that do not permit proper scrutiny also creates uncertainty for relevant operational and oversight agencies, and persons subject to the new powers.

35. These agencies and individuals have been subjected to the burden of participating in not one but three separate inquiries. It is reasonably foreseeable that they will need to divert further resources into implementing future amendments to remediate avoidable deficiencies in the original enactment. The Law Council is therefore concerned that this approach to the development of major national security legislation is an inefficient use of public and parliamentary resources.

[18] The Law Council expressed concerns about major deficiencies in the Australian Security Intelligence Organisation Amendment Bill 2020 (**ASIO Amendment Bill**), in relation to statutory criteria and procedural requirements governing the eligibility, appointment and termination of lawyers as independent 'prescribed authorities' who would supervise compulsory questioning by ASIO. These issues would also arise in relation to the potential appointment of members to a new Investigatory Powers Division of the AAT to authorise the issuing of mandatory industry assistance notices. See further, Law Council of Australia, *Submission to the PJCIS Review of the ASIO Amendment Bill,* (July 2020), pp. 57-61 and recommendations 27-30.

Recommendation 12 – AFP Commissioner's approval of TANs issued by State and Territory police

36. At the public hearing on 27 July 2020, the Shadow Attorney-General, the Hon Mark Dreyfus QC MP, invited the Law Council to comment on INSLM recommendation 12 concerning the repeal of section 317LA of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**). This section prohibits State and Territory police from issuing a TAN to a communications provider without the prior approval of the AFP Commissioner.

Background to recommendation 12

37. Section 317LA of the Telecommunications Act was inserted by Government amendments to the (then) TOLA Bill in December 2018, to implement a recommendation of the Committee in its advisory report on the Bill.[19]

38. The Law Council understands that the Committee's objective was to enable comprehensive oversight of, and appropriate coordination and de-confliction between, TANs issued by multiple Australian police forces. This led the Committee to recommend a mechanism that would give the Commonwealth Ombudsman visibility of TANs sought by all Australian law enforcement agencies, through its oversight of the AFP's approval functions in relation to State and Territory police TANs.[20]

39. However, the INSLM recommended the repeal of section 317LA, as he considered that the performance by the AFP of an approval function was incompatible with the independence of State and Territory police forces.[21]

Law Council views

40. The Law Council supports the Committee's objectives to ensure coordination and consistency of oversight between TANs issued by multiple law enforcement agencies. Inter-agency coordination at the stage of issuing TANs is highly desirable to avoid the risk of oppression to communications providers due to the issuing of duplicative or conflicting notices by multiple agencies.

41. Such coordination is particularly important given that the extensive secrecy obligations imposed on communications providers under Division 6 of Part 15 of the Telecommunications Act could limit their ability to raise concerns about the combined effect of multiple notices, once they are issued by multiple law enforcement agencies. In addition, the ability of Commonwealth, State and Territory oversight agencies to coordinate their respective oversight functions is necessary to facilitate consistent standards of conduct by law enforcement agencies under the assistance regime.

42. However, the Law Council also acknowledges the importance of maintaining the independence of law enforcement agencies from each other, as recognised by the INSLM. As the INSLM further observed, his recommended expansion of the industry

[19] Ibid, recommendation 7.

[20] Parliamentary Joint Committee on Intelligence and Security, *Report on the Review of the TOLA Act* (April 2019), 60 at [1.157].

[21] INSLM Report, 206 and recommendation 12.

assistance regime to law enforcement integrity bodies would make it inappropriate for the AFP to have an approval function in relation to those agencies' TANs.[22]

43. Accordingly, the Committee may wish to consider possible alternative statutory mechanisms to give effect to the objectives that prompted it to recommend the approval mechanism in section 317LA of the Telecommunications Act.

Alternative mechanisms to implement the Committee's policy objectives

44. At the public hearing on 27 July 2020, the Law Council identified three legislative mechanisms that may cumulatively address the Committee's concerns. They are:

- **Information-sharing**—namely, the inclusion of comprehensive and flexible provisions authorising information-sharing between Commonwealth, State and Territory oversight agencies about TARs, TANs and TCNs;
- **Independent issuing**—namely, the INSLM's recommendation to establish an independent issuing body for TANs and TCNs would enable that body to hold a register of all notices sought and issued. The ability to consult this register when assessing applications could assist the new body to avoid issuing notices that would impose conflicting or otherwise oppressive obligations on communications providers; and
- **Issuing criteria**—namely, the inclusion of an additional statutory issuing criterion requiring the issuing body to assess the potential impact of multiple TANs or TCNs on a communications provider.

45. Further details of these suggested measures are outlined below. The Law Council emphasises that the text of any proposed amendments to implement these measures would require thorough consultation and parliamentary scrutiny. This should include consultation on draft provisions with relevant oversight bodies and civil society stakeholders, such as the Law Council, before a Bill is introduced to Parliament.

Mechanism 1 – information-sharing provisions for oversight bodies

46. The permitted disclosure provisions in Division 6 of Part 15 of the Telecommunications Act should enable the comprehensive and flexible sharing of information between all Commonwealth, State and Territory oversight and integrity bodies with responsibilities for agencies that may issue TARs, TANs and TCNs.

47. This would provide a mechanism for oversight agencies to gain comprehensive visibility of the circumstances in which all eligible agencies are issuing or obtaining industry assistance requests or notices. Consistency of oversight could facilitate consistency of agencies' practices, while also maintaining the independence of the oversight bodies and the agencies subject to oversight from one another.

48. The Law Council considers that amendments to information-sharing provisions should not be limited to the conduct of joint inquiries, as was the subject of INSLM recommendation 28.[23] Rather, the amendments should enable the sharing of information between oversight agencies in the performance of all of their functions.

[22] INSLM Report, 206 [10.51].

[23] Ibid, 233-234 and recommendation 28 (explicit power of Commonwealth Ombudsman to undertake joint investigations with State and Territory Ombudsmen and anti-corruption bodies in relation to the industry assistance scheme in Part 15 of the Telecommunications Act).

49. In particular, amendments should clearly authorise the conduct of joint inspections of law enforcement agencies' activities under or in relation to TARs, TANs and TCNs. They should also extend beyond joint oversight activities and permit the ongoing sharing of information collected by one oversight agency that is relevant to the performance by other oversight agencies of their functions. This would include sharing inspection findings or inquiry reports, sharing information obtained during an inspection or an inquiry, and sharing information obtained in a preliminary inquiry conducted by an oversight body to determine whether it should investigate a matter (either on their own motion or in response to a complaint).

Key amendments required to Division 6 of Part 15 of the Telecommunications Act

50. The key amendments required to the existing permitted disclosure provisions in section 317ZF of the Telecommunications Act would be to authorise the 'disclosing' oversight agency to share information in its possession for the purpose of the 'receiving' oversight agency performing its separate oversight functions.

51. Currently, the provisions governing State and Territory oversight bodies only permit disclosures for the purpose of the 'disclosing' oversight body performing its functions.[24] This does not clearly authorise an oversight agency to share information for the purpose of enabling another oversight agency to have visibility of a matter that is, or is likely to be, relevant to the other ('receiving') agency's oversight functions.

52. Further, the permitted disclosure provisions applying to the Commonwealth Ombudsman only appear to allow the disclosure of information about a TAR or a TAN to the State or Territory oversight body that has responsibility for oversight of the particular State or Territory law enforcement agency that issued the TAR or TAN.[25] This does not provide a clear basis for the Commonwealth Ombudsman to undertake broader information-sharing with its State and Territory counterparts, about TARs and TANs issued by other State or Territory law enforcement bodies, for the purpose of facilitating national consistency in the approach to the oversight of TARs or TANs that are directed to the same or similar subject-matter.

53. Consideration should also be given to including the Inspector-General of Intelligence and Security (**IGIS**) in these information-sharing arrangements between oversight bodies, given the increasing interoperability between ASIO and law enforcement operations. Such interoperability is evidenced in the establishment of Joint Counter-Terrorism Teams and the Counter-Foreign Interference Taskforce, which comprise members of law enforcement agencies, ASIO and other government agencies.

Mechanism 2 – establishment of an independent issuing body

54. The INSLM's recommendations for the establishment of an independent issuing body for TANs and TCNs[26] will also enable the creation of a centralised repository or register of all compulsory industry assistance notices sought and issued. This register could be reviewed by individual members as part of their functions in determining applications for TANs and TCNs. This would assist the issuing body to identify and manage potential overlap, duplication or oppression arising from extant or previous TANs or TCNs, if the member was to grant the application before them.

[24] *Telecommunications Act 1997* (Cth), s 317ZF(12D). Cf the provisions in ss 317ZF(5B) and (5C) authorising the Commonwealth Ombudsman to share information with a State or Territory oversight body, for the purpose of the 'receiving' State or Territory body performing its functions in relation to the TAN or TAR.

[25] Ibid, ss 317ZF(5B) and (5C).

[26] See further, INSLM Report, Chapter 11 and recommendations 3-6.

55. The parties to the TAN or TCN application (the agency as applicant and the communications provider as respondent) would have an opportunity to make submissions to the issuing authority on duplication or conflicting obligations arising from multiple notices.

56. Accordingly, if the INSLM's recommendations for the establishment of an independent issuing body are implemented, the establishing legislation should include clear provisions enabling the creation of a register of TAN and TCN requests made to, and issued by, that body. The establishing legislation should also explicitly authorise all members of that independent body to access information held on that register for the purpose of making decisions on applications for TANs and TCNs.

Mechanism 3 – an issuing criterion to assess the impacts of 'multiple powers'

57. The functions of an independent issuing body would be assisted if there was a specific issuing criterion for TANs that required the issuing authority to be reasonably satisfied that the TAN, if issued, would not have an oppressive effect on the designated communications provider. This should cover oppression due to the provider being exposed to multiple, duplicative compulsory assistance notices; and oppression arising from exposure to conflicting obligations under multiple notices.

58. It may be argued that this matter could be taken into consideration in reliance on a general discretion of the issuing authority to consider 'the legitimate interests of the designated communications provider' or 'such other matters (if any) as [the issuing authority] considers relevant' as part of the assessment of whether the requirements of a notice are 'reasonable and proportionate.[27]

59. However, the inclusion of an explicit statutory issuing criterion directed to oppression would facilitate the consistent examination of this factor in all decision-making on applications. It would also ensure that the agency requesting a TAN or TCN includes sufficient particulars of all previous requests and orders made in their applications for further TANs or TCNs in relation to a communications provider.

60. A provider would also have the opportunity to make submissions on oppression arising from multiple notices issued by multiple agencies, without risk of contravening the onerous secrecy provisions in Division 6 of Part 15.

Interaction of the TOLA Act with the EU General Data Protection Regulation

Court of Justice of the European Union decision in 'Schrems II'

61. In considering the interaction between the TOLA Act measures and foreign laws, the Committee may be assisted by a recent judgment of the CJEU in *Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems* ('Schrems II') on 16 July 2020.[28]

62. The CJEU considered Articles 44 and 46 of the GDPR (interpreted in light of Articles 7, 8 and 47 of the *Charter of Fundamental Rights of the European Union*), and ruled that:

[27] Telecommunications Act ss 317P and 317RA (TANs) and ss 317V and 317ZAA (TCNs).

[28] *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Court of Justice of the European Union, C-311/18, ECLI:EU:C:2020:559, 16 July 2020).

(a) the European Commission's adequacy decision for the EU-US Privacy Shield Framework is invalid – on the basis that the access and use of European Union (**EU**) personal data by US public authorities is not restricted in a way that, according to the court, meets requirements which are "essentially equivalent" to EU law. Criticism was levied at the lack of limitations on surveillance, the lack of effective judicial redress and shortcomings in the ombudsperson mechanism. As a consequence, companies must stop data exports from the EU to the US using that export mechanism.[29]

(b) Standard Contractual Clauses (**SCCs**) remain valid, however the CJEU has emphasised obligations on parties to SCCs and Data Protection Authorities which have the potential to restrict when they can be used, including that:

(i) parties to the SCCs must verify on a 'case-by-case basis' whether the law of the data importer ensures adequate protection for personal data, as required by EU law; and

(ii) upon receiving a complaint from a data subject, data protection authorities (**DPAs**) are required to suspend or prohibit a transfer of personal data to a third country where they take the view that, in light of all of the circumstances, the SCCs cannot be complied with.[30]

Implications for the interaction of the TOLA Act with the GDPR

63. The decision in Schrems II has broad consequences for non-EEA jurisdictions and could impact transfers to any non-EEA country that has not achieved adequacy status, such as Australia.

64. While the decision has particular applications for transfers to the US and is very critical of the lack of privacy safeguards, effective redress and proportionality of major US surveillance programs, the Law Council submits this criticism has equal application to the compulsory powers conferred on Australian intelligence and law enforcement agencies, including those in TOLA.

65. In particular, the Law Council notes the following passage, which contemplates the imposition of additional obligations on the recipient of personal data by a receiving country (such as the mandating of decryption by TOLA) as a cause to terminate an agreement facilitating the transfer of data from the EU:

> *Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.*[31]

[29] Ibid, [184] – [185], [191] – [197].
[30] Ibid, [132] – [136].
[31] Ibid, [135].

66. The CJEU went considerable lengths to articulate the reasons for the decision, specifically noting that the absence of 'effective and enforceable data subject rights' for data subjects whose personal data is transferred makes it impossible to meet the requirements of Article 45(2)(a) of the GDPR. (This Article requires that, in its assessment of the adequacy of the level of protection in a third country, the Commission is, in particular, to take account of such data subject rights). In addition, the CJEU reiterated that all assessment is to be made by reference to EU laws and the fundamental rights of data subjects under such laws:

> *Furthermore, the Court has consistently held that the validity of provisions of EU law and, in the absence of an express reference to the national law of the Member States, their interpretation, cannot be construed in the light of national law, even national law of constitutional status, in particular fundamental rights as formulated in the national constitutions.*[32]

67. The clear objective is that there is a 'consistent and homogeneous application of the rules for the protection of the fundamental rights and freedoms of such natural persons with regard to the processing of personal data throughout the European Union, the level of protection of fundamental rights required by Article 46(1) of that regulation must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter'.[33]

68. The principled approach to privacy and data protection (as fundamental rights) by the European Union, together with this decision, cast further doubt on the possibility of Australia achieving 'essential equivalence' or allowing it to achieve adequacy status for the purpose of negotiating an agreement for the importation of data from the EU, because of the lack of privacy safeguards provided for the use of the powers in TOLA.

69. These potential criticisms are not limited to Schedule 1, and could also be directed at the expansion of computer access warrants to intercept telecommunications as well as existing concerns regarding the lack of independent authorisation of these powers.

[32] Judgments of 17 December 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, paragraph 3; of 13 December 1979, Hauer, 44/79, EU:C:1979:290, paragraph 14; and of 18 October 2016, Nikiforidis, C-135/15, EU:C:2016:774, paragraph 28 and the case-law cited therein.

[33] Ibid, [100]

Appendix 1

Law Council of Australia response to INSLM recommendations and outstanding issues on the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)

Contents

Schedule 1 – Industry assistance scheme: *Telecommunications Act 1997* (Cth), Part 15

INSLM recommendations on Schedule 1 (recs 1-12 and 25-31)

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
Recommendation 1 – extension of industry assistance scheme to anti-corruption agencies I recommend that State and Territory anti-corruption commissions be given power to agree to or apply for all 3 types of industry assistance notice – that is, TARs *[Technical Assistance Requests]*, TANs *[Technical Assistance Notices]* and TCNs *[Technical Capability Notices].* This power should also be given to the foreshadowed Commonwealth Integrity Commission, when and if it is established. *INSLM report, pp. 204-206, [10.43]-[10.52].*	**Support, contingent on the implementation of INSLM recommendations 2-12 and 25, 31, and the outstanding issues identified by the Law Council (see below)** The Law Council acknowledges that the INSLM found that anti-corruption and law enforcement integrity agencies faced the same challenges as law enforcement and security agencies, arising from the use of encryption by the targets of their investigations. However, necessity alone is not conclusive of whether it is appropriate to extend the compulsory industry assistance powers to State and Territory anti-corruption bodies. The INSLM found that the industry assistance scheme is not, in its present form, proportionate to the legitimate investigative objectives to which it is directed, and that substantial amendments were needed. Accordingly, the Law Council's support for INSLM recommendation 1 is contingent on implementation of all of the INSLM's recommended amendments to the industry assistance scheme. The Law Council's support for this recommendation is also contingent on implementation of its recommendations on outstanding issues not addressed by the INSLM.
Recommendation 2 – TARs I recommend no change to the capacity of the relevant agencies and a DCP [Designated Communications Provider] to freely agree a TAR with each other, other than that a prescribed form be used. *INSLM report, pp. 203-204 at [10.38]-[10.42].*	**Support, contingent on implementation of the outstanding issues identified by the Law Council below** The Law Council does not object in principle to an appropriately targeted statutory immunity scheme to encourage communications providers to give voluntary, request-based technical assistance to law enforcement, anti-corruption and intelligence agencies. However, the Law Council considers that additional and clearer statutory parameters are needed to ensure the proportionality of agencies' powers under TARs to grant civil immunities and criminal immunities from computer offences. (See details of the Law Council's recommendations in the 'outstanding issues' section below.) At the absolute minimum, it is critical that TARs are subject to a statutory maximum period of effect (for example, 90 days would be consistent with TANs).

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
Recommendations 3-6 – issuing of TANs and TCNs by a new Investigatory Powers Division of the AAT ***Recommendation 3 – issuing authority*** I recommend that the powers of approval of TANs and TCNs, presently vested in agency heads (for TANs) and the Attorney-General (for TCNs), instead be vested in the AAT and assigned to a new Investigatory Powers Division (IPD). The new IPD, building on the powers and procedures in the Security Division, would operate in a similar way to protect classified material of agencies that are applying for TANs and TCNs and the commercial-in-confidence material of DCPs that are resisting the issue of those notices. The IPD should be able to sit in private as necessary. It would be able to utilise existing AAT powers and procedures, including alternative dispute resolution, to decide for itself whether to issue a TAN or TCN. It would hear submissions and receive evidence from the applying agency and the DCP and be in a position to promptly determine technical questions, such as whether a notice is practicable, reasonable and proportionate or would create a systemic weakness. The Attorney-General's approval would be required for a federal agency to lodge an application for a TCN with the AAT, but this should not be required for any State or Territory body or the Commonwealth Integrity Commission, if and when it is established. *INSLM report, pp. 211-212 at [10.70]-[10.73]; and Chapter 11 (in entirety)*	**Support in principle** The Law Council strongly supports the conferral of an issuing function on an authority that is independent of security and law enforcement agencies and ministers. The Law Council also considers it essential that the independent issuing authority is given full access to independent technical expertise to assist its decision-making. The Law Council also acknowledges that conferring the issuing function on a body, rather than individuals, may facilitate deeper expertise and consistency of decision-making. However, several matters require further attention: • **Nature of the issuing function and the responsible body**—further consideration should be given to conferring a judicial authorisation function on a court, rather than conferring an administrative function on a division of the AAT. This would, of course, require consideration of constitutional issues, and practical issues arising from requirements of open justice and the application of the rules of evidence. However, as the INSLM acknowledged, these issues are not insurmountable obstacles. The Law Council considers that the interests of independence, both substantive and perceived, are significant benefits of conferring a judicial authorisation function on a court that merit further consideration. • **Possible additional functions of an independent issuing body**—in designing an independent body for issuing TANs and TCNs, consideration should be given to the potential to expand the body's functions in future (for example, the issuing of International Production Orders, and potentially all Commonwealth intelligence or evidence collection warrants). • **Safeguards for independence if functions are to be conferred on a new division of the AAT**—if there is an appetite to create a specialist division of the AAT rather than a court, the INSLM's recommendations 4-6 about appointments (eligibility, qualifications and aspects of the process) **must** be implemented, **as a baseline.** In addition, there must be: o an open and transparent appointment process, which includes consultation with the legal profession (including the Law Council) as well as industry; o statutory appointment criteria that prescribe the expertise and seniority of members of the new division (including significant experience in criminal law); o robust provisions to disqualify people from appointment if they have an actual, potential or perceived conflict of interest (including a conflict arising from past and current employment; and in the case of part-time appointments, their future employment, if known at the time of their potential appointment to the AAT); and o extensive consultations on proposals for the new body, including the Law Council.

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
Recommendation 4 – Investigatory Powers Commissioner I recommend that the IPD consist of a new part-time Deputy President, who would also be the Investigatory Powers Commissioner (IPC), and other eminent lawyers and technical experts as needed. So that they can build up the necessary specialised expertise, and because these powers will not be exercised *ex parte*, the exercise of these powers should not be *persona designata*. *INSLM report, chapter 11 (in entirety)*	**Support in principle** – as per recommendation 3 above.
Recommendation 5 – Additional functions of Commissioner I recommend the creation of the IPC as a new statutory office holder, whose functions would be: (a) monitoring the operation of TOLA [Telecommunications and Other Legislation Amendment Act] Schedule 1, including by sharing information with other oversight bodies (such as the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman) and reporting annually on its operation to the Attorney-General and the PJCIS [Parliamentary Joint Committee on Intelligence and Security] (b) as an additional, part-time Deputy President of the AAT, taking part in the issue of TANs and TCNs as head of the IPD (c) concurring in the appointment of other part-time technical and legal decision-makers assigned to the new IPD who will also be able to assist the IPC in the monitoring roles (d) developing and approving the prescribed form for TAR, TAN and TCN applications and issuing guidelines (e) with the concurrence of the AAT President, issuing practice notes for the IPD *INSLM report, chapter 11 (in entirety)*	**Support in principle** – as per recommendation 3 above.

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
Recommendation 6 – Appointment of Commissioner In recognition of the importance of the IPC and the need for the role to be, and be seen to be, filled by someone who is independent of government, is eminent in the law and its application, enjoys bi-partisan support and is not diverted by judicial duties, I recommend that the IPC be a retired judge of the Federal Court or the Supreme Court of a State or Territory, appointed by the Governor-General, on the advice of the Attorney-General, following mandatory consultation on the appointment with the Leader of the Opposition. I would expect there would also be consultation with industry, but I would not mandate it. *INSLM report, chapter 11 (in entirety).*	**Support in principle** – as per recommendation 3 above.
Recommendation 7 – definitions of 'serious offences' for the purpose of law enforcement agencies' TARs, TANs and TCNs I recommend amending the definitions in TOLA of 'serious Australian offence' and 'serious foreign offence' so that they align with the definition in existing s 5D of the [*Telecommunications (Interception and Access) Act 1979* (Cth)] TIA Act. The effect of this is that, by and large, it would not be open to an agency to obtain an industry assistance notice in respect of an offence punishable by only 3 years' imprisonment. *INSLM report, pp. 234-237 at [12.31]-[12.43].*	**Support** This recommendation endorses the Law Council's suggestions to the INSLM and the Committee. The Law Council remains of the view that the present threshold for a 'serious Australian offence' or a 'serious foreign offence' in s 317B of the Telecommunications Act is too low (being an offence punishable by a maximum penalty of at least three years' imprisonment, or life). The Explanatory Memorandum to the TOLA Bill indicated, at paragraph [4], that the powers conferred by the industry assistance regime were intended to target the investigation of offences relating to terrorism or child exploitation. In fact, the definition of a 'serious offence' vastly expands the number of applicable offences and could be used against individuals suspected of committing relatively minor criminal offences. The INSLM concurred with the Law Council's assessment that this is not proportionate. As the INSLM noted, the threshold for a serious offence under the TIA Act is generally an offence punishable by a maximum penalty of at least seven years' imprisonment, as well as other individually listed offences, and offences constituted by conduct that involves, or would involve, loss of life, serious personal injury, property damage in circumstances endangering the safety of a person, serious fraud, bribery or corruption. If the industry assistance scheme is amended to apply the TIA Act definition of a 'serious offence', the Law Council notes that any future amendments to the TIA Act definition will need careful scrutiny with a view to assessing their impacts on the industry assistance scheme. The Committee may wish to draw this matter to the attention of the Parliament as a matter requiring ongoing legislative scrutiny, including by legislative scrutiny committees.

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
Recommendations 8-9 – definition of 'systemic weakness' and 'systemic vulnerability' ***Recommendation 8 – systemic vulnerability*** As to systemic weakness and vulnerability, I recommend removing all references to 'systemic vulnerability' in Schedule 1, as it is redundant. *INSLM report, pp. 207-209 at [10.55]-[10.58]*	**Support** This recommendation is consistent with the concerns the Law Council raised with the INSLM and Committee about the vague and ambiguous nature of the concept of 'systemic vulnerability' for the purpose of the prohibition on matters that may be requested under a TAR or compelled under a TAN or TCN in s 317ZG.
Recommendation 9 – 'systemic weakness' I recommend that s 317ZG(4A) state prohibited effects as follows: (4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection means a reference to any act or thing that creates a material risk that otherwise secure information will be accessed, used, manipulated, disclosed or otherwise compromised by an unauthorised third party. I further recommend the introduction of the following definitions: (a) 'Otherwise secure information' means 'information of, any person who is not the subject, or is not communicating with the subject of, an investigation'. (b) 'Unauthorised third party' means 'anyone other than a party to the communication, the agency requesting the relevant TAR, TAN or TCN and/or integrity agencies'. *INSLM report, pp. 207-209, [10.55]-[10.58]; pp. 210-211, [10.65]-[10.68]*	**Support** This recommendation endorses an alternative recommendation of the Law Council to address the vague and potentially indeterminate meaning of a 'systemic weakness' The Law Council's preferred reform to section 317ZG is that there should simply be a prohibition on a TAR, TAN or TCN being used to request or require a communications provider to introduce or fail to remediate **any** weakness in a system of product. However, if the concept of a 'systemic weakness' is to be retained, the Law Council supports the INSLM's recommended amendments to improve its clarity. In particular, INSLM recommendation 9 would define component terms, in relation to the part of the definition of a 'systemic weakness' that covers the introduction of a 'selective weakness' to a 'target technology' that is 'connected with a particular person'. The INSLM's recommended definitions of the terms 'otherwise secure information' and 'unauthorised third party' endorse suggestions made by the Law Council to the INSLM and the Committee.
Recommendation 10 – use of statutory examples I recommend clarification of definitions through the use of non-exhaustive statutory examples: (a) Clarify that 'target technology' in s 317B refers to the specific instance used by the intended target.	**Support** This recommendation is consistent with the Law Council's position that there is a need for statutory clarity on the meaning of the component terms within the concept of 'systemic weakness' in section 317ZG (if the concept of a 'systemic' weakness is to be retained, although this is not the Law Council's preferred option as noted above). The Law Council emphasises the importance of consultation with industry and civil society, including the Law Council, on draft statutory examples before a Bill is introduced to Parliament.

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
(b) Include non-exhaustive examples of what is excluded from the meaning of 'electronic protection' in s 317B. *INSLM Report, pp. 209-210 at [10.59]-[10.64]; p. 230 at [12.14]-[12.15]*	
Recommendation 11 – Designated Communications Providers (DCPs) as bodies corporate I recommend that a 'Designated Communications Provider' not be taken to include a natural person (where that natural person is an employee of a DCP) but only apply to natural persons insofar as required to capture sole traders.	**Support** This recommendation would address concerns raised by many industry members to the INSLM and the Committee inquiries. It would give express statutory effect to the policy intent identified by the Department of Home Affairs during the INSLM inquiry that individual employees of a corporate entity should not be restricted from telling their employer about a TAN or TCN addressed to them individually. The Law Council supports the view of the INSLM that legislative amendments are needed to remove any possibility for any legal ambiguity or doubt to arise, and to provide industry with a clear legal assurance that it is lawful and proper for employees of a body corporate to disclose such information to their employer, and the secrecy offences will not apply to such actions.
Recommendation 12 – AFP approval of State/Territory police TANs I recommend that the AFP no longer have any role in the consideration of industry assistance notices requested by or issued on behalf of State and Territory police. *INLSM Report, p. 206 at [10.53].*	**Support, with further amendments to enable de-confliction of TAN requests made by multiple agencies, and comprehensive oversight by multiple agencies** The Law Council acknowledges the conclusion of the INSLM that the requirement in s 317LA for the AFP Commissioner to approve TANs of State and Territory police, before they could be issued to providers, is incompatible with the independence of State and Territory police forces. However, the Law Council remains supportive of the objective of the Committee to ensure coordination and consistency of oversight over TANs made by multiple law enforcement agencies, which led it to recommend the enactment of this provision in 2018. As noted in the Law Council's evidence at the Committee's public hearing on 27 July 2020 (and explained in main body of this submission), the Law Council supports amendments to Part 15 of the Telecommunications Act to give effect to the Committee's objective in a different way. These amendments are directed to: • **independent issuing**—amendments are needed to ensure that the independent issuing body (per INSLM recommendations 3-6) maintains, and is able to use in their decision-making on applications, a register or repository of all TAN and TCN applications and notices, so as to identify and manage risks of duplication, conflict or oppression to communications providers arising from multiple notices directed to the same or similar subject-matter; • **issuing criteria**—amendments are needed to the issuing criteria for TANs and TCNs to require the issuing authority to assess the potential for the TAN or TCN sought to have an

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
	oppressive effect on the communications provider, including as a result of conflict with, or duplication of, current or previous notices issued to the provider at the request of the applicant or any other agency; and • **coordination and consistency of independent oversight**—amendments are needed to enable multiple oversight bodies (such as the Commonwealth, State and Territory Ombudsmen) to undertake joint and coordinated oversight activities of the agencies within their respective jurisdictions, including by sharing information with each other. See further details in the in the main body of this submission.
Recommendation 25 – Record-keeping and reporting I recommend that relevant agencies keep a record of the number of industry assistance orders that are executed and provide them annually to the IPC. *INSLM report, pp. 231-232 at [12.16]-[12.21]*	**Support** The collation of statistical and other information about the operation of the industry assistance scheme will provide an important evidence base to assess its operation in future (including its continued necessity and proportionality by the INSLM and the Committee). In the interests of transparency and public trust and confidence, this recommendation should be implemented in combination with INSLM recommendation 26, for the public reporting of aggregated statistical information, and a broad description of the acts or things done.
Recommendation 26 – Statistical reporting I recommend that the various industry assistance order provisions be amended to mandate that the agency in question report to its oversight agency (such as the Commonwealth Ombudsman or the IGIS) as to the number of assistance orders that it executes each year and, other than for ASIO, publish those figures in the public annual reports of the relevant agencies and the oversight bodies. I recommend that statistics on the use of TOLA powers, including a broad description of the acts or things implemented, be made public annually by the IPC (tabled in Parliament within 15 sitting days of receipt) provided that publication would not reveal operationally sensitive or classified information. *INSLM report, pp. 231-232 at [12.16]-[12.21]*	**Support** This recommendation endorses the Law Council's suggestion for greater public reporting not only of statistical information, but also descriptions of the types of acts or things done under the industry assistance scheme. The Law Council considers that there should be precisely defined tests for the exclusion of information from such reporting, particularly any proposals to withhold statistical information. The Law Council continues to support a review by the INSLM or the Committee of whether there is a continuing requirement for ASIO to enjoy a wholesale exemption from any public annual reporting of statistical information about the majority of its warrant or authorisation-based intelligence-collection powers (as recommended in the Law Council's submission to the Committee's present review of the Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020). This review should consider the approaches taken by other, comparable countries to the release of statistical information on their intelligence agencies' use of intrusive powers, including the United Kingdom.

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
Recommendation 27 – section 313 assistance requests I recommend that agencies be required to keep records of the number of requests they make of carriers or carriage service providers under s 313 of the Telecommunications Act and to report on those matters annually to the IPC. *INSLM report, p. 234 at [12.30].*	**Support** The Law Council considers that a requirement for agencies to collate statistical information pm their use of s 313 requests is valuable to monitor the operation of that separate assistance regime. Further to this, establishing the IPC (or another independent issuing body) to act as a centralised repository of information about the exercise of **multiple powers** will also be valuable, as it will give that body visibility of the way in which agencies are utilising the full suite of legislative tools available to them to address the problem of targets 'going dark'. This will desirably give the new body an awareness of the broader operational context in which it performs its authorisation functions for industry assistance notices (and any other functions that may be conferred on it in future, such as other warrants and international production orders). In addition to the implementation of INSLM recommendation 27, the Law Council also supports the public release of aggregated statistical information on the use of s 313 in the annual report of the IPC (or such other independent body upon which the issuing function may be conferred).
Recommendation 28 – Joint oversight activities I recommend that the capacity of the Commonwealth Ombudsman to undertake a joint investigation with State Ombudsmen or Independent Commission Against Corruption oversight bodies such as Inspectors-General be made explicit within s 317ZRB of the Telecommunications Act. *INSLM report, pp. 233-234 at [12.29].*	**Support** The Law Council considers that independent oversight bodies must have a clear ability to conduct joint oversight activities. Joint oversight is a necessary corollary of the increasing interoperability between law enforcement and intelligence agencies, especially their frequent use of joint operations (such as the use of Joint Counter-Terrorism Teams and the establishment of the national Counter-Foreign Interference Taskforce). However, the Law Council considers that provisions enabling cooperative oversight need to extend more broadly than joint investigations or inquiries, and should cover the joint performance of **all oversight functions** of these agencies (such as inspections, and preliminary inquiries to determine whether to commence an investigation into a matter). In addition, there should be adequate provision for information-sharing between oversight bodies, for purposes of assisting each other in the performance of their individual functions, and ensuring visibility of the wider operational context in which individual law enforcement agencies are utilising the industry assistance scheme. Further, in view of increasing interoperability between law enforcement and intelligence agencies, the Law Council recommends that consideration is given to including the IGIS in cooperative and information-sharing provisions. In addition to the need for amendments to s 317ZRB of the Telecommunications Act identified by the INSLM, amendments will also be required to the disclosure provisions in s 317ZF.

INSLM recommendation – Schedule 1 (recommendations 1-12 and 25-31)	Law Council response
Recommendation 29 – Commonwealth Ombudsman reports As to the Commonwealth Ombudsman's powers of reporting, I recommend that s 317ZRB(7) be repealed so that the Minister cannot remove material from an Ombudsman report under that provision. *INSLM report, pp. 237-239 at [12.43]-[12.49].*	**Support** This recommendation endorses suggestions by the Law Council, which supported the submissions of the Commonwealth Ombudsman, to remove the power of Ministerial redaction in relation to the Ombudsman's reports on its oversight of the industry assistance regime. This is necessary to ensure the independence of the Ombudsman, which is critical to public trust and confidence in the lawful operation of the industry assistance regime.
Recommendation 30 – Permitted disclosures by agencies I recommend that Commonwealth officials be authorised to disclose TAR/TAN/TCN information to the public and to State, Territory and Commonwealth officials when that disclosure is in the national or public interest. A decision to disclose based on those factors may be made by the relevant agency or departmental head or the relevant minister. *INSLM report, p. 232 at [12.24]-[12.25].*	**Support** It is important that the disclosure provisions in section 317ZF of the Telecommunications Act do not prevent the pro-active disclosure of information pertaining to a TAR, TAN or TCN where there is a public interest in doing so. However, the Law Council considers that INSLM recommendation 30 should be supplemented with a request-based mechanism, so that DCPs and others (such as journalists or industry bodies) can request the relevant officials to make a public disclosure of information. This would be analogous to the approval-based permitted disclosures for DCPs in existing ss 317ZF(14)-(16) but would cover requests for the information to be disclosed to the **public at large**, not just individual persons or entities such as contracted service providers to the DCP. There should also be external merits review rights for officials' decision-making on requests for disclosure (as part of or analogous to FOI laws).
Recommendation 31 – permitted disclosures for the purpose of a DCP obtaining technical advice I recommend that the information disclosure provisions be amended so as to permit DCPs to obtain not merely legal advice but also technical advice in relation to the request or potential request of TARs and the issue or potential issue of TANs and TCNs. *INSLM report, p. 233 at [12.26]-[12.28].*	**Support** The Law Council considers it appropriate that the statute removes any ambiguity or doubt about the rights of a DCP to obtain technical assistance to ascertain whether it is technically feasible to implement a TAR, TAN or TCN, and the implications of doing so. It is conceivable that the ability of a DCP to understand their legal position and obtain effective and useful legal advice may require technical advice about the feasibility of the request or requirement. Clarity about the ability of a DCP to make disclosures in connection with technical advice is essential in view of the disclosure offences in Division 6 of Part 15.
Conclusion at [12.5], p. 229 I conclude that there be developed prescribed forms for TARs, TANs and TCNs, to be approved by the Investigatory Powers Commissioner (IPC) and used when the Administrative Appeals Tribunal (AAT) is issuing TANs and TCNs; and that each prescribed form set out the recipient's rights and obligations, and any other important information specific to the TAR, TAN or TCN in question. *INSLM report, pp. 228-229 at [12.1] -[12.5]*	**Support** This recommendation endorses a suggestion of the Law Council that a person must be informed of their rights to make complaints to the relevant independent oversight body responsible for the agency, in relation to all industry assistance requests and notices. The Law Council considers that there should be consultation with industry and civil society, including the Law Council, on the suite of prescribed forms before they are finalised.

Outstanding issues in relation to Schedule 1

Summary of Law Council recommendation / comment (per previous submissions to the PJCIS and INSLM)	Law Council comment on the continuing need for amendments

Issuing criteria for TARs, TANs and TCNs:
 	
Statutory guidance on the 'reasonable and proportionate' test' (ss 317JC, 317RA and 317ZAA)
 	
• The test should specifically require the decision-maker to determine whether perceived law enforcement imperatives demonstrably outweigh the reasonable expectation of confidentiality in electronic communications between individuals and businesses.
 	
• The test should also:
  ○ include guidance on how the individual factors are to be weighed or balanced when considering whether a notice 'is reasonable and proportionate';
  ○ include a higher threshold of 'significant or serious' national security and law enforcement interests at paragraphs 317JC(a)–(b), 317RA(a)–(b), 317ZAA(a)–(b);
  ○ specify that the 'legitimate interests of the DCP to whom the notice relates' include commercial interests at paragraphs 317JC(c), 317RA(g), 317ZAA(c) to;
  ▪ omit from paragraphs 317JC(i), 317RA(g), 317ZAA(g) 'such other matters as the Director-General of Security or the chief officer, as the case requires, considers relevant';
  ▪ insert 'or' or 'and' after each matter listed;
  ▪ refer explicitly to the fundamental human right to privacy; or alternatively, refer to the Australian Privacy Principles under the Privacy Act and the potential privacy impact of a TAN or TCN be evidenced by a privacy impact assessment undertaken by the OAIC;
  ○ refer explicitly to a requirement of proportionality;
	The Law Council continues to support amendments to ss 317JC, 317RA and 317ZAA to provide greater statutory guidance to the relevant decision-makers (and affected parties) in applying the 'reasonable and proportionate' requirement for issuing a TAR, TAN or TCN, as recommended in the Law Council's previous submissions to the Committee and the INSLM.
	
	In particular, the Law Council notes the following matters:
	
	The need for a high degree of statutory guidance on the application of the test to TARs, by intelligence and law enforcement agencies
	
	This is especially important for TARs, which will continue to be authorised internally by law enforcement and security agencies (and will be expanded to anti-corruption bodies, if INSLM recommendation 1 is implemented).
	
	The power to confer a civil immunity, and immunity from criminal liability to computer offences, is very significant – especially because third parties whose rights to a remedy may be extinguished are unlikely to know of the TAR and have an opportunity to make known and protect their interests. This warrants a higher degree of statutory guidance and prescription about the application of the issuing test, to ensure that it is consistently and accurately applied by the multiple decision-makers, across multiple agencies. This will also help to facilitate compliance and therefore reduce the need for major remedial action if defects in the exercise of broad discretionary criteria are identified via independent operational oversight carried out by the IGIS or relevant Ombudsman.
	
	The desirability of providing statutory guidance on the application of the test to TANs and TCNs, by the independent issuing body (per INSLM recommendations 3-6)
	
	The Law Council's recommended amendments in relation to the issuing thresholds for TANs and TCNs are also important to facilitate consistency and clarity in requests and decision-making on TANs and TCNs (and oversight by the IGIS and relevant Ombudsmen of agencies' requests). This is not diminished by the appointment of an independent issuing authority.

Summary of Law Council recommendation / comment (per previous submissions to the PJCIS and INSLM)	Law Council comment on the continuing need for amendments
○ include factors which require the issuer of a TAR, TAN or TCN to separately consider the potential legal consequences to the recipients of warrants; and ○ require the decision maker to determine whether use of the measure is necessary in the investigation or enforcement of laws in relation to investigation or enforcement of a serious offence in circumstances where imperatives of law enforcement demonstrably outweigh reasonable expectations of confidentiality in communications of affected individuals and businesses. • The threshold for issuing a TAN or TCN should also import a broader 'less intrusive' or 'less restrictive' test, which should relate to surveillance capabilities to obtain the information through other means – not simply through industry assistance.	
Scope of the prohibition on 'systemic weaknesses' Subsection 317ZG(1) should be amended to prohibit a TAR, TAN or TCN from requesting or requiring anything that might require a DCP to either implement or build [or fail to remediate] any weakness into a current or proposed product or service [not limited to a form of electronic protection]	The Law Council remains of the view that the prohibition is unduly narrow, in that it is limited to the introduction or non-remediation of a systemic weakness into a form of **electronic protection only,** and not all of the products or services that are utilised in a communications supply chain in entirety. The Law Council remains concerned that the limited scope of the current prohibition may make it possible for TARs to request, or TANs and TCNs to compel, the installation of software or hardware that is subject to a backdoor or other vulnerability; or the modification or substitution of a service to remove features that prevent decryption. The Law Council's recommendation would be consistent with the intent of recommendation 10 of the Committee in its review of the (then) TOLA Bill in December 2018 to expand the coverage of the prohibition. The Committee recommended that the prohibition on a systemic weakness or vulnerability in s 317ZG(1) should extend to all 'listed acts or things' in s 317ZE. This recommendation does not appear to have been implemented. However, to ensure that the prohibition applies comprehensively, the Law Council considers it would be preferable for s 317ZG(1) to refer to all products and services generally, rather than relying on the definition of enumerated 'listed acts and things' as in force from time-to-time. Further, the Law Council considers it important that the prohibition covers 'proposed' products and services, to ensure that it covers unreleased products and services that are being developed by a DCP at the time the TAR, TAN or TCN is issued.

Summary of Law Council recommendation / comment (per previous submissions to the PJCIS and INSLM)	Law Council comment on the continuing need for amendments
'Relevant objectives' that a TAR, TAN or TCN must support There should be amendments to the requirements in ss 317G(2), 317L(2) and 317T(3) for the assistance sought under a TAR, TAN or TCN to relate to the performance of a function, or the exercise of a power by a law enforcement or intelligence agency, in relation to a relevant objective. These amendments should remove the provisions in ss 317G(2)(a)(vi), 317L(2)(d) and 317T(3)(b)(ii) which allow a TAR, TAN or TCN to request or compel assistance that **merely facilitates or is ancillary or incidental** to the performance of a function or the exercise of a power by an agency, that relates to a relevant objective.	The Law Council continues to support the limitation of the industry assistance regime to assistance that is directly relevant to the performance by an agency of its functions or the exercise of its powers in relation to a 'relevant objective'. The Law Council considers that the provision of assistance that is merely ancillary, incidental or facilitative is disproportionate to the magnitude of the powers to confer civil immunities and immunities from computer offences (and to extinguish third parties' rights to remedies) and to compel private entities to render assistance to the state.
Maximum duration of TARs TARs should be subject to a maximum time limit, after which a new TAR would have to be sought and issued [subject to the Law Council's further recommendations about a statutory cap on the number of consecutive TARs, TANs and TCNs that may be issued in relation to the same assistance.]	The Law Council continues to support a statutory maximum time limit on the assistance that can be requested (and given civil immunity and immunity from computer offences) under a TAR. This is necessary to reflect the extraordinary nature of the power conferred on agencies to self-authorise the granting of legal immunities, and to ensure its proportionality. The Law Council considers that the requirements of proportionality necessitate a legal safeguard (in the form of a prohibition) against the use of TARs to confer indefinite, indeterminate or prolonged immunities on DCPs (thereby extinguishing the rights of third parties to legal remedies in respect of loss, harm, damage or injury suffered). A statutory maximum duration for TARs would ensure that, if the agency considers there is a need for the assistance to continue, it must make a new TAR request and the issuing criteria would be assessed afresh.
Limitation of TARs and TANs to a single instance of assistance TARs and TANs should not be capable of authorising the ongoing provision of the specified assistance [in the nature of a 'standing' request or requirement that can be called in by the agency at-will] and should cease to be in force once a single instance of assistance has been provided.	The Law Council remains of the view that the Telecommunications Act should expressly remove the possibility for a TAR or a TAN to be issued that requests or compels (and confers immunity for) assistance on a standing basis, which can be 'called-in' by an agency at-will. Conferring discretion on an agency to request or compel 'standing' assistance is not proportionate to either the extinguishment of third party rights to legal remedies as result of the attendant civil immunity; or the compulsory nature of TANs. Rather, each repetition of the relevant act of assistance should be requested or compelled under a new TAR or TAN, so that each instance of the assistance sought is subject to the separate application of the issuing test.

Summary of Law Council recommendation / comment (per previous submissions to the PJCIS and INSLM)	Law Council comment on the continuing need for amendments
Assistance that can be requested under a TAR The list of 'acts and things' [that can be requested under a TAR] at subsection 317G(6) should be amended to replace the words 'but are not limited to' with 'must be' as has been done for subsections 317L(3) and 317T(7) [in relation to the things that can be compelled under a TAN or TCN].	The Law Council remains of the view that there is no rational basis for allowing TARs to request, and confer immunities in relation to, a potentially indeterminate range of acts or things. It continues to support consistency across all forms of industry assistance This would implement the Committee's recommendation 10 in its advisory report on the TOLA Bill in December 2018, which was not limited only to TANs and TCNs.
Limitations on civil and criminal immunities ***Civil immunity*** INSLM recommendation 20 (exclusions from the civil immunity under s 21A of the ASIO Act) should apply equally to the civil immunities conferred by TARs, TANs and TCNs. That is, the civil immunities would not apply to conduct resulting in serious personal injury or death to any person, or significant loss of, or serious damage to, property. There should also be an express statutory provision indicating that 'significant loss of property' includes financial loss (or an additional reference to financial loss should be included). ***Criminal immunities – computer offences*** Subsection 476.2(4) of the *Criminal Code Act 1995* (Cth) (**Criminal Code**) should be amended to provide that an act done under a TAR, TAN or TCN that has no legal effect (for example, because it breaches a prohibition on the matters that can be requested or compelled) will not be conferred criminal immunity from the computer offences in the Criminal Code.	The Law Council remains of the view that the scope of the civil immunities conferred under the industry assistance scheme and s 21A of the ASIO Act should be aligned. The Law Council also remains of the view that the immunity from criminal liability for a computer offence should explicitly extend only to a TAR, TAN or TCN that was valid; or at least to those instances in which the DCP believed on reasonable grounds that the TAR, TAN or TCN was valid.
Monitoring, reporting and notification requirements on the enlivenment of civil immunities Agencies should be required to notify the relevant oversight body (the relevant Ombudsman or the IGIS) if they become aware that a DCP has done an act or a thing under a TAR, TAN or TCN, and has caused loss, damage or harm to another person. Consideration should be given to a requirement that at least ASIO, ASIS and ASD should report the matter to their ministers. Further consideration should be given to annual reporting on these matters.	The Law Council remains of the view that the enlivenment of civil immunities conferred under TARs, TANs and TCNs should be kept under close scrutiny by oversight agencies and their Ministers. A notification requirement would provide an effective and efficient way of focusing oversight on this matter. This recommendation would have the further, beneficial effect of requiring agencies to take all reasonable steps to monitor the execution of TARs, TANs and TCNs by the relevant DCPs (this may include, for example, provisions in notices or accompanying contracts requiring DCPs to inform the agency).

Summary of Law Council recommendation / comment (per previous submissions to the PJCIS and INSLM)	Law Council comment on the continuing need for amendments
Removing ambiguity in the prohibitions in s 317ZH Subsections 317ZH(4)(e) and (f) should be amended to make explicit that a TAR, TAN or TCN cannot request or require a DCP to do an act or a thing for which the relevant agency would require a warrant or another form of statutory authorisation or approval. Rather, a TAR, TAN or TCN can only request or require a DCP to **facilitate or assist** the agency to execute a warrant or authorisation that has already been issued, and is in force. If there is an appetite to utilise the industry assistance scheme to request or require a DCP to do an act or a thing that is authorised under a warrant **that has already been obtained and is in force**, then that DCP must be separately authorised (under the relevant legislation) to exercise authority under that warrant (for example, under s 24 of the ASIO Act or s 19 of the TIA Act). That is, the industry assistance scheme should be capable of operating to displace these separate authorisation requirements.	The Law Council remains concerned that s 317ZH(4)(f) is ambiguous, and in fact creates doubt rather than achieving the stated policy objective of avoiding doubt. In particular, the Law Council is concerned that this provision may be open to interpretation as creating an exception to the prohibition in s 317ZH(1). This risks creating a perverse incentive for agencies to use the industry assistance scheme to bypass separate warrant and authorisation requirements. The Law Council considers that this risk should be removed through clearer drafting that removes the ambiguity and consequent risks of misuse or non-compliance. As the IGIS identified in previous evidence to the Committee, the most straightforward way of addressing this issue would be to simply remove s 317ZH(4)(f) from the Act.
Technical Capability Notices (TCNs) • **Acts or things required to be done by a DCP:** Any addition to the list of acts or things that can be specified in a TCN should be by legislative amendment (which would remove the delegated legislative power enabling the Minister to add matters by legislative instrument). Alternatively, if it is to remain by legislative instrument, subsection 317T(6) should be amended so that the Minister is required to explicitly consider the potential impact on human rights, such as the right to privacy, as a condition of exercising delegated legislative power. • **Replacement TCNs:** Subsections 317W(7) and (8) should be removed in order to eliminate the potential that a DCP may receive a 'replacement TCN' without their approval. • **Technical feasibility assessments:** The assessment report under subsection 317WA should be binding on the Attorney-General. That is, the Attorney-General must not proceed to give a TCN unless each assessor is satisfied with the matters set out in subsection 317WA(7) • **Approval:** Section 317TAAA should be amended so that the Minister, when considering whether to approve the issuance of a TCN, is required	The Law Council continues to support the implementation of these measures, to ensure appropriate Parliamentary control over the scope of the TCN regime, and procedural fairness in its application. However, if INSLM recommendations 3-6 are implemented to establish an independent issuing body for TANs and TCNs, the Law Council's recommendations in points 3-4 at left (technical feasibility assessments and approval) will require the modifications below: **Variations to reflect the appointment of an independent issuing body (INSLM recs 3-6)** • **Technical feasibility assessments**—the independent issuing body should not be permitted to issue a TCN contrary to advice of the appointed technical expert members that the requested capabilities would not be technically feasible, or would involve the creation or non-remediation of a systemic weakness. • **Approval—**if there is to be a 'double lock' authorisation requirement (whereby the an agency must obtain the approval of the Attorney-General to make an application to the independent issuing body for a TCN) then the Attorney-General and the independent issuing authority must consider the **same** criteria in performing their respective functions. (That is, it **should not** be the case that some matters are reserved only to the Attorney-General in deciding whether to approve an agency to make an application.) ***[Continued]***

Summary of Law Council recommendation / comment (per previous submissions to the PJCIS and INSLM)	Law Council comment on the continuing need for amendments
to apply the decision-making criteria contained in sections 317JAA, 317P and 317V, and consequently, be required to consider the same matters listed in sections 317JC, 317RA, 317ZAA, to ensure the issuance of the TCN is reasonable and proportionate.	Other than these variations, the establishment of an independent issuing body (as recommended by the INSLM) does not remove the need for the Law Council's recommendations at left to be implemented. The Law Council's recommendations are consistent with the overriding theme in the INSLM's report that there should be clear and certain legal limitations on the power to issue a TCN, and the things that can be compelled under a TCN, to ensure that there is a reasonable basis for public trust in agencies' activities.
Exceptions to disclosure offences • Disclosure of TAR, TAN or TCN information to the Office of the Australian Information Commissioner (**OAIC**) and the Australian Commissioner for Law Enforcement Integrity (**ACLEI**) should be deemed an authorised disclosure under subsection 317ZF(3). • There should be a defence to the unauthorised disclosure of information in accordance with the *Public Interest Disclosure Act 2013* (Cth) (**PID Act**) or the *Freedom of Information Act 1982* (Cth) (**FOI Act**).	The Law Council remains concerned about the gaps it has previously identified to the INSLM and Committee in the protections for permitted disclosures under Division 6 of Part 15 of the Telecommunications Act The Law Council's recommended amendments would simply bring Division 6 of Part 15 of the Telecommunications Act into line with the approach to exceptions to the official secrecy offences in Part 5.6 of the *Criminal Code Act 1995* (Cth). (The Committee specifically recommended that Part 5.6 of the Criminal Code cover these matters.) Currently, the exceptions in Part 15 of the Telecommunications Act only cover disclosures to and by IGIS and Ombudsman officials, whereas the exceptions in Part 5.6 of the Criminal Code cover all of the matters identified in the Law Council's recommendations (at left). It is important the legislation provides explicit confirmation that it is lawful and appropriate for public officials to make disclosures in accordance with the PID Act and FOI Act; and for DCPs and DCPs and public officials to make disclosures to the OAIC and ACLEI; and for the OAIC and ACLEI to make subsequent disclosures for the purpose of performing their functions. The absence of explicit provisions to this effect may create legal uncertainty or complexity. Irrespective of the ultimate, technical legal construction of how the different sets of provisions interact, the mere existence of uncertainty due to the absence of a clear pathway for disclosure on the face of the Telecommunications Act, could create a disincentive to people coming forward to OAIC or ACLEI, or making public interest disclosures under the PID Act (as applicable). This was the reason that the Committee recommended that Part 5.6 of the Criminal Code contain comprehensive exceptions.
Elements of disclosure offences The offence in s 317ZF(1) should include an express harm requirement.	The Law Council remains of the view that disclosure offences applying to persons who are **not** members of law enforcement or intelligence agencies should require proof of the harmful effects of disclosures (or likely harmful effects) and require the discloser to intend or be reckless as to the effect or likely effect of their disclosure.

Summary of Law Council recommendation / comment (per previous submissions to the PJCIS and INSLM)	Law Council comment on the continuing need for amendments
DCP requests to make disclosures Section 317ZF should be amended so that a request for disclosure from a DCP must be authorised unless it would prejudice an investigation, a prosecution or national security. *[See ss 317ZF(14)-(17).]*	The Law Council continues to support amendments to ensure that secrecy obligations are limited only to those circumstances in which disclosure would be reasonably likely to cause harm. This will ensure that the obligations do not go any further than is necessary and proportionate to protect legitimately sensitive information. The Law Council's recommended amendments at left would ensure that there is no discretion to withhold information in circumstances in which disclosure would not cause significant harm to security or law enforcement interests.
Re-issuing of expired TARs, TANs and TCNs Sections 317HA, 317HA and 317TA should be amended to include a limit on the number of fresh notices or requests that can be issued.	The Law Council continues to support amendments to the total duration a DCP can be requested or compelled to provide assistance. This is important to ensure the proportionality of the power to confer civil immunities and criminal immunities from computer offences, and the corresponding extinguishment of third parties' rights to legal remedies for consequent harm, loss, damage or injury. In particular: **For TARs—**a statutory cap on the **total duration** of a request (across multiple, consecutive instruments) is particularly important given that these instruments (and therefore decision-making about the conferral of civil immunities and immunities from computer offences) are internally authorised. **For TANs and TCNs** – the Law Council acknowledges that the INSLM's recommendations 3-6 for the independent issuing of TANs and TCNs may assist in avoiding oppression to DCPs and third parties whose rights to remedies are being extinguished by civil immunities. However, there remains a risk that an effectively uncapped maximum duration (via the unlimited re-issuing of consecutive notices in the same terms as an expired notice) could operate oppressively, especially to third parties, who would not be parties to the application and could not be informed of the application (or the issuing of the TAN or TCN). **Alternative measures to facilitate proportionality of the total duration of an assistance request or notice (including the attendant immunities from legal liability)** If there is no appetite to place a cap on the total number of requests or notices for the same form of assistance, then as a minimum, the agency issuing a TAR or the authority issuing a TAN or TCN, should be required to specifically consider the proportionality of the total duration of the assistance, across **all** of the individual, consecutive TARs, TANs or TCNs. This should require consideration of the impacts on all third parties for the total duration (ie, the end users of communications systems or services; and 'downstream' participants in the communications supply chain). This should be supported by a requirement for the applicant to give the decision-maker details of all previous TAR, TAN and TCNs sought and issued.

Summary of Law Council recommendation / comment (per previous submissions to the PJCIS and INSLM)	Law Council comment on the continuing need for amendments
Rights of DCPs to compensation for compliance with TANs and TCNs Section 317ZK should be amended to confer a statutory right to compensation (on a 'no profit and no loss' basis) for all DCPs who comply with TANs and TCNs. The relevant agency head or Attorney-General should not have discretion to effectively 'turn off' that right on the basis of their opinion that it would not be in the public interest to pay such compensation to the DCP.	The Law Council remains of the view that that the threshold for 'turning off' a DCP's statutory right to compensation for acts or things done under a TAN or TCN is too low, and should not be self-assessed by agencies or the Attorney-General. The Law Council remains concerned by the potential risk that it could be determined that the interests of law enforcement and national security outweigh the regulatory burden on the DCP, because it is in the interests of the agencies or the government more generally to divert their resources into its other efforts in law enforcement and national security.
Defences to the penalty provisions for non-compliance with TANs and TCNs, in relation to contraventions of foreign laws Subsection 317ZB(5) should be amended to expand the defence to civil penalty proceedings for a DCP's failure to comply with a requirement under a TAN or TCN, on the basis that doing the relevant act or thing **in a foreign country** would contravene the law of the foreign country. The defence should be available irrespective of the geographical location in which the DCP does the act or thing. Rather, it should be available in all circumstances in which the DCP is subject to the jurisdiction of the foreign country, not only in relation to acts or things done outside Australia.	The Law Council remains of the view that the defence should not be limited to acts or things done outside Australia, thereby excluding acts or things done inside Australia despite the DCP being subject to the extraterritorial jurisdiction of the foreign country. Problematically, the current scope of proposed s 317ZB(5) means that a DCP's obligation to comply with a TAN or TCN may bring them into conflict with a foreign law that prohibits the relevant act or thing. (For example, Article 32 of the EU General Data Protection Regulation obliges the controllers and processors of personal data to implement appropriate technological and organisational measures to ensure an appropriate level of security, including the encryption of personal data.) Further, the Law Council remains concerned that it is extremely difficult to ascertain the geographical location in which a particular act or thing is done, having regard to the transnational operation of the technology that a TAN or TCN may target. For example, it is conceivable that a TAN or TCN may require a DCP operating in Australia to do an act or thing in Australia, but the software may be located or partially located in a foreign country or is executed or modified remotely from Australia. In such circumstances, it may be factually impossible to ascertain where the act was done (that is, in Australia or the foreign country). The Law Council considers that the defence, in its present form, is defective because it fails to take account of both extraterritorial jurisdiction of foreign countries, and factual indeterminacy arising from the transnational nature of communications technologies. Framing the defence in this limited way is also out-of-step with modern legislative practice – including the US CLOUD Act and the Australian Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020 – which seeks to avoid conflicts of law.

Schedules 2-4 – Computer access warrants (law enforcement agencies and ASIO) and search warrants and mandatory assistance orders (law enforcement agencies)

INSLM recommendations on Schedules 2-4 (recs 13-18 and 32)

INSLM recommendation on Schedules 2-4 (recommendations 13-18 and 32)	Law Council response
Recommendation 13 – Telecommunications interception (TI) powers under computer access warrants I recommend that agencies retain the power to engage in limited telecommunications interception, for the purposes of a computer access warrant, without the need to obtain a separate warrant under the TIA Act authorising that interception. *INSLM report, pp. 239-240 at [12.50]-[12.55].*	**The Law Council supports the retention of a TI power as part of computer access warrants, subject to amendments to limit the purpose for which it may be exercised** The Law Council does not oppose the conferral of a TI power as part of a computer access warrant, provided that the power can only be exercised for the purpose of ASIO accessing relevant data held on, or accessible from, a computer. The Law Council notes that this purpose was the stated policy intent for integrating a TI power into computer access warrants, but the provisions of the ASIO Act and the SDA authorise a much broader application. ***Overbreadth of the TI power under computer access warrants*** For example, it would be possible to intercept a telecommunication under a computer access warrant for the purpose of ASIO or a law enforcement agency to gain access to premises: see ASIO Act ss 25A(aa) and (aaa) and SDA, ss 27E(2)(a) and (b). (For instance, accessing the content of the text messages or voice calls of an occupant of the premises on which a computer is located, to determine the movements of that person and others to and from the premises, to assess whether the warrant can be executed covertly at a particular time.) In its submission to the Committee in the present inquiry, the Department of Home Affairs indicated that it envisaged that the TI power would only be used 'rarely' for purposes other than accessing relevant data, and made a general appeal to a desire for operational flexibility as the basis for retaining the broader availability of a TI power to all of the things that are authorised under a computer access warrant in addition to accessing relevant data. The Law Council considers that a vague appeal to operational flexibility is an inadequate justification for the conferral of a TI power for purposes beyond gaining access to relevant data under a computer access warrant. ***The broad power for secondary use of TI obtained under computer access warrants*** A limitation on the purposes for which TI can be carried out under a computer access warrant is particularly important in view of the extremely broad secondary uses that can be made of TI information collected under a computer access warrant. ***[Continued]***

INSLM recommendation on Schedules 2-4 (recommendations 13-18 and 32)	Law Council response
	For example, under ss 63AB and 63AC of the TIA Act, ASIO and law enforcement agencies can make secondary use of such TI information if it relates, or appears to relate, to the involvement of a person in: • activities that are, or are likely to be, a threat to security (within the meaning of that term under the ASIO Act); • activities that are a significant risk to a person's safety; • acting for or on behalf of a foreign power; and • activities that relate to the proliferation of weapons of mass destruction, or the contravention of UN sanctions. The first permitted use (concerning actual or likely security threats) would appear to cover most of ASIO's investigative functions, and most law enforcement investigations into security offences. As such, sections 63AB and 63AC fail to apply a significant break to the ability of agencies, especially ASIO, to make secondary use of TI information obtained under a computer access warrant. It is therefore essential that the scope of the TI power is limited.
Recommendation 14 – concealment of computer access I recommend that an agency be required to seek external authorisation to exercise a concealment of access power if it proposes to take that step more than 28 days after the warrant has expired. *INSLM report, pp. 240-241 at [12.56]-[12.63]*	**Support** This recommendation is consistent with the Law Council's suggestions to the INSLM and Committee. It addresses concerns raised by the Law Council that the post-warrant concealment powers are disproportionate because they authorise the exercise of highly intrusive powers for a prolonged, and potentially indefinite, period after the warrant has expired. In particular, the Law Council notes that the task of erasing or concealing a digital footprint may be considerably more difficult than the concealment of physical surveillance activities. It is conceivable that it will be necessary for ASIO or a law enforcement agency to undertake ongoing activities to conceal, and thereafter continue to conceal from other computer users, the fact that relevant data was copied, modified or deleted from a computer under the authority of a computer access warrant.
Recommendation 15 – temporary removal of computers and other things from warrant premises I recommend that the legislation be amended to require that a computer or thing which is removed from warrant premises during the execution of a computer access warrant (or related authorisation) be returned to warrant	**Support** The INSLM's recommendation addresses the concern underlying the Law Council's recommendation for maximum a time limit on the temporary removal of a computer or other thing from premises, to avoid indeterminate or prolonged retention. ***[Continued]***

INSLM recommendation on Schedules 2-4 (recommendations 13-18 and 32)	Law Council response
premises if returning the computer or thing is no longer prejudicial to security or, otherwise, as soon as is it reasonably practicable to do so. *INSLM report, pp. 242-243 at [12.64]-[12.69].*	The INSLM concurred with the Law Council's concern that there are no statutory mechanisms in the ASIO Act or SDA to ensure that a computer or other thing is not removed from premises for a longer period of time than is necessary to do an act or thing under the computer access warrant (for example, to access and copy relevant data) and to effect the (covert) return of the computer or thing. While a fixed maximum period of removal would provide the greatest degree of clarity and certainty, a 'reasonably practicable' threshold would nonetheless make it unlawful for an agency to retain a computer or other thing longer than is necessary to do the things authorised under a warrant. What constitutes the first 'reasonably practicable' opportunity to return an item would require determination in individual cases (and review as part of oversight by the IGIS and Ombudsman). This makes it important that agencies have clear policies and make adequate records of their decision-making on this matter, to facilitate both compliance and oversight.
Recommendation 16 – breach of assistance orders: *Crimes Act 1914* (Cth), section 3LA; *Customs Act 1901* (Cth) s 201 and *Australian Security Intelligence Organisation Act 1979* (Cth), section 34AAA I recommend that agencies and external stakeholders continue to monitor the prosecutions and convictions (to the extent that information is made publicly available) so as to permit any trends to be discerned as more time passes. *INSLM report, pp. 246-248 at [12.86]-[12.95]*	**Support** To the extent possible, the Law Council, as an external stakeholder, will monitor this matter. However, there should be a central coordination point within the Government to perform this function, such as the Commonwealth Director of Public Prosecutions. Further, the relevant governmental coordination point should also provide the INSLM with periodic updates for the purpose of their annual reports and broader current awareness. (The Law Council understands this is the established practice with respect to terrorism prosecutions and the exercise of other preventive and disruptive powers.)
Recommendation 17 – Assistance orders do not authorise detention I recommend that both s 3LA of the Crimes Act and s 201A of the Customs Act be amended to state, for the avoidance of doubt, that neither authorises the detention of a person to whom the order applies where the agency in question does not otherwise have any lawful basis to detain the person. *INSLM report, pp. 255-257 at [12.125]-[12.134].* *See also recommendation 23 (equivalent for orders under ASIO Act s 34AAA)*	**Support** The INSLM acknowledged, and sought to address in recommendation 17, the Law Council's concerns that mandatory assistance orders could be executed in a way that amounts to the arbitrary detention of a person who is required to attend a place to render assistance to a law enforcement agency. This is particularly because there are no statutory maximum periods for a person's attendance to render assistance (where this is required under an order) and a person is liable to criminal penalty if they left the place without attempting to provide the assistance. INSLM recommendation 17 would make clear that any actions purportedly authorised in an order, or taken in purported compliance with an order, that in substance amounted to detention would be beyond power and therefore unlawful.

INSLM recommendation on Schedules 2-4 (recommendations 13-18 and 32)	Law Council response
Recommendation 18 – penalty for offence of deliberate non-compliance with a mandatory assistance order under the Crimes and Customs Acts I recommend that a monetary penalty be retained as an alternative to a penalty of imprisonment for failing to comply with an industry assistance order. *INSLM report, pp. 248-249 at [12.96].*	**Support** The Law Council does not object to the retention of the existing pecuniary penalty provisions, the enforcement of which should be kept under review, including by the INSLM, as part of the implementation of INSLM recommendation 16 (see above).
Recommendation 32 – record-keeping and statistical reporting requirements for assistance orders that <u>are not</u> executed I recommend that there is no need to keep any record of, or to report on the number of assistance orders that an agency issues but which are ultimately not executed. *INSLM report, pp. 245-246 at [12.79]-[12.85].* **Additional conclusion – record-keeping and reporting requirements for assistance orders that are executed** I conclude that relevant agencies should keep a record of the number of assistance orders that are executed and provide them annually to the IPC. *INSLM report, p. 245 at [12.80].*	**Support** The Law Council has no objection, in principle, to the INSLM's view that a discrete statutory record-keeping and reporting obligation for these orders may not be essential to the performance by law enforcement agencies of their functions. However, INSLM recommendation 32 should not be interpreted as relieving agencies of **all** record-keeping obligations in relation to assistance orders that are obtained but not ultimately executed. In particular, agencies' obligations under Commonwealth, State and Territory record-keeping legislation of general application should continue to apply – for example, under the *Archives Act 1983* (Cth). Further, agencies should maintain adequate records to ensure that independent oversight bodies (such as Ombudsmen) can conduct oversight activities as needed. The Law Council notes that this could potentially include oversight of agencies' decision-making about whether to seek an assistance order and the terms of that order, and whether to execute it.

Outstanding issues in relation to Schedules 2-4

Summary of Law Council recommendation / comment (per previous submissions to the INSLM and PJCIS)	Law Council comment on the continuing need for amendments
Emergency authorisations under the SDA Section 32 of the *Surveillance Devices Act 2004* (Cth) (**SDA**) should be amended to state that telecommunications intercepts will not be permitted under emergency authorisations, consistent with the former subsection 32(4) of the SDA.	The Law Council remains concerned that law enforcement agencies will be able to self-authorise telecommunications intercepts under an emergency authorisation (that is, without independent authorisation as would be required under a warrant). No explanation or justification has been given for this devolution in the level of authority. In the absence of a cogent justification, this power should not be retained.
Disclosures about law enforcement computer access warrants for the purpose of obtaining legal advice The SDA should be amended to permit disclosures about computer access warrants under Division 4 Part 2 of the SDA for the purpose of obtaining legal advice.	The Law Council notes that information obtained by a law enforcement agency under a computer access warrant, and information about the existence of that warrant, would be 'protected information' under s 44 of the SDA. This would enliven the offences in s 45 for unauthorised disclosures, which apply to 'a person' not merely 'entrusted persons' to whom information has been lawfully disclosed by a law enforcement agency subject to conditions, restrictions or prohibitions on subsequent disclosure (cf s 18(2) of the ASIO Act). The Law Council is concerned that there is only an exception in s 45(2)(a) of the SDA for information that has been disclosed in court. This does not cover disclosures for the purpose of obtaining legal advice before legal proceedings have been commenced. The Law Council acknowledges that it may be unlikely that a person will become aware that their computer has been accessed under a warrant (since they are intended to be used covertly). However, if for any reason a person becomes aware of such a warrant, they should be able to obtain independent legal advice about their rights, especially if they have suffered harm or damage, which they believe is a result of the execution of the computer access warrant. (For example, there may be circumstances in which a law enforcement agency decides it is necessary to make a disclosure about the existence of a warrant; or a person may detect that access has been gained to their computer if concealment efforts are unsuccessful.)

Summary of Law Council recommendation / comment (per previous submissions to the INSLM and PJCIS)	Law Council comment on the continuing need for amendments
Other matters concerning the scope of TI, temporary removal and use of force powers under computer access warrants (Schedule 2) The LCA submissions to the PCIS raised a number of other issues in relation to schedule 2 (and also schedule 5, as to which, see the separate tables below). Most of these endorsed technical issues identified in the IGIS submissions to the PJCIS reviews of the TOLA Bill and Act. *(See, eg: LCA submission to the PJCIS, TOLA Bill (Oct 2018), pp. 33-47.)* Key issues pertaining to Schedule 2 (computer access warrants) include: • limiting the power to intercept telecommunications under a computer access warrant to the purpose accessing relevant data held in, or accessible from, a computer (and **not** for the purpose of doing any of the things authorised under the warrant, such as entering premises); • a prohibition on the use of force (which was currently authorised under ASIO's computer access warrants prior to the TI-related amendments) for the purpose of carrying out TI (as distinct to other activities authorised under the warrant, such as gaining access to premises); • limiting the power to temporarily remove a computer or other thing from premises to the purpose of accessing relevant data, and not any of the other acts that can be authorised under a warrant. (For example, it should not be possible to remove a set of keys from the premises on which a computer is located, in order to facilitate entry and exit to the premises for the purpose of executing the warrant); • clearly specifying what 'other things' can be temporarily removed from premises (for example, a requirement that the thing must have a direct connection with a computer – such as a data storage device or another peripheral piece of equipment); • a requirement for ASIO to report to the IGIS, and law enforcement agencies to report to the Ombudsman, on **all instances** of temporary removal of computers or things from premises (not only if ASIO or the law enforcement agency assesses that the removal causes material interference, loss or damage). This is necessary to ensure that effective independent oversight can be carried out in relation to ASIO and law enforcement agencies' decision-making about whether a removal caused a material interference, or material loss or damage;	These issues remain unresolved. The Law Council continues to support their further consideration by the Committee in the present inquiry. It further supports legislative amendments to give direct effect to as many of these as possible (rather than dealing with them in administrative guidelines, which are not a legal safeguard and are vulnerable to unilateral repeal or amendment).

Summary of Law Council recommendation / comment (per previous submissions to the INSLM and PJCIS)	Law Council comment on the continuing need for amendments
• an additional statutory issuing criterion that requires an assessment of the privacy impacts on the proposed computer access (particularly in relation to the privacy of third parties who may use the computer); and • stronger safeguards on computer access warrants issued for the purpose of Australia executing a mutual assistance request received from a foreign government, in cases that involve the investigation or enforcement of offences carrying the death penalty.	

Schedule 5 – ASIO civil immunities and mandatory assistance orders

INSLM recommendations on Schedule 5 (recs 19-23 and 33)

INSLM recommendation on Schedule 5 (recommendations 19-23 and 33)	Law Council response
Recommendation 19 – ASIO power to confer civil immunity to persons who are requested to give voluntary assistance (ASIO Act, s 21A) I recommend that the power to request conduct in s 21A(1) be limited in scope to the conduct which can be volunteered under s 21A(5) *[That is, the power to confer a civil immunity would be limited to requesting people to provide documents and information to ASIO, for the purpose of assisting ASIO to carry out any of its functions. ASIO would not have the power to confer a civil immunity on people who it requests to engage in any kind of conduct – at ASIO's complete discretion – for the purpose of assisting ASIO to carry out its functions.]* *INSLM report, pp. 249-251 at [12.100]-[12.106]*	**Support** The INSLM concurred with the Law Council's view that the breadth of the ASIO's power to confer civil immunities in subsection 21A(1) is not necessary or proportionate. (Currently, that provision authorises ASIO officials to confer a civil immunity on any person who engages in any kind of conduct, at ASIO's request, for the purpose of assisting ASIO in the performance of any of its statutory functions under s 17 of the ASIO Act.) In combination, INSLM recommendations 19 and 20 (see below) would address the Law Council's concerns, subject to a clarification that significant financial loss is excluded from the immunity (see recommendation 20 below).
Recommendation 20 – exclusions from the civil immunities in s 21A I recommend that s 21A(1)(e) and s 21A(5)(e) be amended to confine the scope of that immunity from civil liability by requiring instead that 'the conduct does not result in ***serious personal injury or death to any person*** or significant loss of, or serious damage to, property' (emphasis added). *INSLM report, pp. 252-253 at [12.107]-[12.113]*	**Support, subject to express statutory clarification that 'significant loss of property' includes financial loss (or the insertion of a separate reference to financial loss)** This recommendation endorses a suggestion of the Law Council. However, for the avoidance of doubt, the Law Council considers that the exclusions from civil liability should expressly cover significant financial loss (that is, 'pure economic loss' that does not involve the destruction of, or damage to, physical property). If there is an intention to invest ASIO with the power to grant civil immunities for actions that cause significant financial loss (for example, to the extent of bankruptcy), then a compelling policy justification should be provided for the necessity of this power. It would also be necessary to increase the level of authorisation, and the applicable authorisation thresholds, to ensure that the exercise of the power to confer civil immunity for such loss is proportionate to the legitimate objectives (if established) to which that power is directed. In combination with INSLM recommendation 19 (above), these amendments would address the Law Council's concerns about the overbreadth and disproportionality of ASIO's power in s 21A(1) to confer a civil immunity on people who provide assistance to ASIO, on its request, which can comprise any kind of conduct for the purpose of assisting ASIO to perform any of its functions.

INSLM recommendation on Schedule 5 (recommendations 19-23 and 33)	Law Council response
Recommendation 21 – level of authorisation for s 21A(1) immunities I recommend that s 21A arrangements be approved by the Director-General of Security or a Deputy Director-General. *INSLM report, p. 253 at [12.114]-[12.117]*	**Support, contingent on implementation of INSLM recommendations 19, 20, 22 and 33** The Law Council's preferred option is that the power to confer a civil immunity should be vested in the Attorney-General, consistent with the level of authorisation for ASIO's special intelligence operations (which can also confer civil immunity on participants, as well as criminal immunity). However, if INSLM recommendations 19, 20, 22 and 33 are implemented to significantly restrict the scope of the civil immunity and strengthen reporting requirements, then the Law Council would not object to the devolution of authority to the Director-General or a Deputy Director-General. While the scope of the civil immunity would be more limited, the power to confer an immunity from civil liability is nonetheless extraordinary. Presently, the ASIO Act authorises all 'senior position holders' in ASIO (effectively senior executive level officials) to exercise the power in s 21A(1) to confer a civil immunity. The INSLM concurred with the Law Council's concerns that this devolution of authority is not proportionate to the extraordinary nature of the power, which could extinguish the rights of third parties to a legal remedy for loss, harm or damage. Concerningly, the power is presently conferred on **all officers** of a senior executive (or equivalent) classification within ASIO. This includes those in non-operational roles (such as human resources, finance, media or policy) who would not necessarily have the requisite operational knowledge and visibility, or decision-making skills in an operational context.
Recommendation 22 – removing overlap between civil immunities under s 21A and Technical Assistance Requests I recommend that s 21A of the ASIO Act be amended to make clear that nothing in s 21A authorises the Director-General of Security to make a request of a person that is properly the subject of a TAR. *INSLM report, pp. 254-255 at [12.118]-[12.124]*	**Support** This endorses a suggestion of the Law Council, to remove duplication between two powers to confer civil immunities that were subject to different authorisation thresholds, limitations, and reporting requirements. The Law Council also raised concerns with the INSLM and Committee about the potential for s 21A immunities being used by ASIO to bypass warrant requirements. (For example, ASIO recruiting and tasking human sources to obtain information, which would not have been an offence or a civil wrong for that person, but would have been for ASIO.) Implementation of INSLM recommendation 19 (see above) would go a considerable way towards managing this risk, as it would limit the conduct able to be immunised under a s 21A(1) request. (That is, the INSLM recommended that s 21A(1) should only enable ASIO to make requests for information or documents, not any conduct.) ***[Continued]***

INSLM recommendation on Schedule 5 (recommendations 19-23 and 33)	Law Council response
	The need for close oversight of the propriety of ASIO's decisions to use s 21A(1) However, the Law Council emphasises the importance of the IGIS being adequately resourced to conduct oversight of the propriety of ASIO's decision-making about its collection methods. (That is, the propriety of ASIO's decision-making about whether to exercise the power in s 21A(1) to recruit, task and confer civil immunity on human sources who may have lawful access to information; as opposed to ASIO directly collecting that information under a special powers warrant authorised by the Attorney-General. These collection methods, for the same intelligence, involve significantly different levels and thresholds of authorisation.) A hypothetical example of the type of decision-making that would require close scrutiny for propriety issues could be any decision-making by ASIO to focus its efforts on recruiting (as human sources) people who live, work or socialise with the targets of investigations, in order to use the immunity power in s 21A(1) to task them with obtaining information or documents possessed by the target, which are located in a shared place of work or residence, to which the human source (but not ASIO) has lawful access. In this type of scenario, propriety concerns could arise if the threshold for ASIO obtaining a warrant (such as a computer access, surveillance or search warrant) to directly collect the relevant material could not be met. This may indicate that the immunity is being used to circumvent those thresholds. The potential for propriety risks to arise in this context also underscores the importance of ASIO adopting and consistently implementing sound record-keeping practices in relation to its decision-making about whether to exercise the power in s 21A(1) to confer a civil immunity on a person. It also heightens the importance of implementing INSLM rec 21 to limit the power to confer immunities to the Director-General or Deputy Director-General of Security.
Recommendation 23 – assistance orders under s 34AAA of the ASIO Act do not authorise detention I recommend that the ASIO Act be amended so as to expressly state, for the avoidance of doubt, that the power does not authorise the detention of a person to whom the order applies where ASIO does not otherwise have any lawful basis on which to do this. *[**See also:** rec 17 on AFP and Customs assistance orders, under s 3LA of the Crimes Act and s 201 of the Customs Act.]* *INSLM report, pp. 255-257 at [12.125] to [12.134].*	**Support** This recommendation addresses concerns raised by the Law Council that the lack of statutory safeguards applying to section 34AAA of the ASIO Act (and equivalent orders for law enforcement agencies under the Crimes Act and Customs Act) created a risk that mandatory assistance orders could arbitrarily detain a person who is required to attend a place to render assistance to ASIO to make certain data intelligible. This is particularly because there are no statutory maximum periods of attendance, and a person is liable to a criminal penalty for failing to comply with the order if they sought to leave without attempting to provide the assistance specified in the order. The INSLM's recommended amendment would make explicit that any actions purportedly authorised under an order, or taken in purported compliance with an order, that in fact amounted to detention would be unlawful. ***[Continued]***

INSLM recommendation on Schedule 5 (recommendations 19-23 and 33)	Law Council response
	It will be important to ensure that the IGIS is adequately resourced to conduct oversight of ASIO's use of mandatory assistance orders, and that adequate records are kept by ASIO about the execution of those orders.
Recommendation 33 – annual reporting on s 21A civil immunities and s 34AAA assistance orders I recommend that ASIO's exercise of powers under Schedule 5 be detailed in its annual report (in a classified appendix as necessary) and that this information be provided to the PJCIS, the Leader of the Opposition, the IGIS, the INSLM, the Attorney-General and the Minister for Home Affairs.	**Support** The Law Council supports comprehensive annual reporting requirements on the use by ASIO of its power to confer civil immunities and compel assistance to make intelligible the data it has obtained under its warrants. The Law Council considers it particularly important that the INSLM and Committee are kept apprised of the use of these powers, in order to monitor the ongoing necessity, proportionality and efficacy of these measures, including their compliance with human rights. However, the Law Council considers that the case for ASIO being subject to a wholesale exemption on public statistical reporting requires review. The Law Council has raised this question in in multiple recent submissions to the Committee on other legislative proposals concerning ASIO, including the ASIO Amendment Bill 2020, and the Telecommunications and Other Legislation Amendment (International Production Orders) Bill 2020. The Law Council has recommended that the PJCIS review, or refer to the INSLM for review, the basis for the wholesale suppression of statistical information on ASIO's special powers an Telecommunications Interception warrants and other authorisation-based powers (such as telecommunications data access).

Outstanding issues in relation to Schedule 5

Summary of previous Law Council recommendation / comment (per previous submissions on the Committee)	Law Council comment on the continuing need for amendments
Other matters in LCA submission to PJCIS on the TOLA Bill (Oct 2018) The LCA submissions to the PCIS raised a number of other issues in relation to Schedule 5. Most of these endorsed technical issues identified in the IGIS submissions to the PJCIS reviews of the TOLA Bill and TOLA Act. *(See, eg, LCA submission to the PJCIS on the TOLA Bill (Oct 2018), pp. 49-55.)* Key issues pertaining to Schedule 5 (ASIO powers) include: • Subsection 21A(1) request-based immunities should be: o subject to a maximum period of effect; o subject to an express statutory issuing criterion directed to assessing the reasonableness and proportionality of the request for voluntary assistance, including the impact of the civil immunity on third parties whose rights to legal remedies will be extinguished; o incapable of immunising the repeated provision of the same act of assistance (that is, a 'standing request' that continues indefinitely or for a prolonged period). Rather, a fresh s 21A request must be made for each act of assistance; o subject to express statutory provisions governing variation and revocation; and o subject to statutory notification requirements to the Attorney-General and IGIS, if ASIO becomes aware that the person providing voluntary assistance exceeds the limitations of the civil immunity. There should be a corresponding statutory obligation on ASIO to make all reasonable efforts to monitor the conduct of the person upon whom ASIO has conferred immunity under s 21A(1). • Section 34AAA compulsory assistance orders should be: o required, <u>in all cases</u>, to specify essential details such as the time and place of attendance or deadline for giving information (as applicable) not merely if a computer has been removed from premises;	The Law Council continues to support the inclusion of all of these measures in the ASIO Act. In particular, while the Department of Home Affairs has noted in previous submissions to the Committee and the INSLM that the Government is considering addressing at least some of these issues through amendments to the ASIO Guidelines made under s 8A of the ASIO Act, the Law Council considers that all of these issues need to be addressed in primary legislation. This reflects that the ASIO Guidelines are merely administratively binding on ASIO, which means that the consequences for non-compliance are merely administrative (such as Ministerial reprimand, internal disciplinary action against individual ASIO officers by the Director-General of Security, and adverse advisory findings by the IGIS). The ASIO Guidelines do not place a legal limitation on the power of ASIO to confer civil immunities, or the power of the Attorney-General to issue compulsory assistance orders. As such, mere administrative requirements in the ASIO Guidelines, which are vulnerable to unilateral repeal or amendment by the Minister for Home Affairs, are not legal safeguards that limit the availability of these extraordinary powers to confer immunities or compel assistance. Further, the Law Council is concerned that the prolonged inaction in making critical amendments to the ASIO Guidelines (despite multiple recommendations of the Committee for at least the past six years) means that the public and the Parliament do not have a reasonable basis on which to be assured that the Guidelines would be updated in a timely way. In particular, the Law Council notes that the TOLA measures have been operational since December 2018, yet no amendments to the Guidelines have been made to address matters arising from the TOLA Act. The Law Council is also concerned that the Department of Home Affairs indicated to the Committee, in its evidence on the ASIO Amendment Bill 2020, that it does not consider it necessary to consult with civil society, including the Law Council, on revisions to the ASIO Guidelines. (See: Proof Committee Hansard, 10 July 2020, 58.) The Law Council submits that the absence of a participatory, transparent and timely process for administratively managing these outstanding concerns lends further support to a case for dealing with these matters via legislative amendments.

Summary of previous Law Council recommendation / comment (per previous submissions on the Committee)	Law Council comment on the continuing need for amendments
○ subject to statutory notification or service requirements, including obligations to explain the effect of the order to the person; and ○ subject to an issuing criterion that requires the Attorney-General to consider the potential for oppression to the person subject to the order, as a result of the exercise of multiple coercive or intrusive powers. (For example, the Attorney-General should be informed about previous s 34AAA orders; questioning warrants; TANs or TCNs; and should be required to consider this as part of the issuing decision). • Further, there should be statutory clarification of the interaction of compulsory assistance orders under s 34AAA with ASIO's questioning warrants. (That is, where a person who is attending for questioning under an ASIO questioning warrant is issued with a s 34AAA assistance notice during their attendance.) For example, questions will arise about whether: ○ compulsory questioning under the questioning warrant may or must be paused for the purpose of executing the assistance order; ○ the time a person spends complying with the assistance order should be offset against the maximum questioning period under the questioning warrant, in recognition that the person is under coercion; and ○ the legal power of IGIS officials (who are in attendance to supervise compulsory questioning under the questioning warrant) attending the execution of the assistance order at the place of questioning.	

Independent National Security Legislation Monitor Act 2010 (Cth)

INSLM recommendation (rec 24)

INSLM recommendation (recommendation 24)	Law Council response
Recommendation 24 – INSLM review functions over TOLA amendments I recommend that the definition of 'counter-terrorism and national security legislation' in s 4 of the INSLM Act be amended to include TOLA so that future INSLMs may review it of their own initiative as necessary. *INSLM report, pp. 184-187 at [9.17]-[9.26].*	**Support** This amendment will ensure that the amendments made by the TOLA Act can be reviewed holistically by the INSLM in future, including on their own motion or on the referral of the Parliamentary Joint Committee on Intelligence and Security. There may otherwise not be a clear statutory basis under the INSLM Act for comprehensive oversight of the continued necessity and proportionality of the TOLA measures – particularly where the powers are used in the investigation of non-terrorism or security-related offences. Further, as the third INSLM noted in his report, this amendment would enable a future INSLM to revisit the conclusions in the current report from time-to-time. It would also provide a future INSLM with a clear basis for monitoring implementation of the recommendations in the third INSLM's report. The Law Council is also supportive of a further statutory review of the TOLA amendments by the Committee, once they have been in force for a further period of time. This further Parliamentary review could potentially be informed by a prior referral by the Committee to the INSLM (which would require implementation of INSLM recommendation 24 in order for the INSLM to have jurisdiction over the TOLA Act in entirety).