Law Council
OF AUSTRALIA

Statutory review of Part 14 of the *Telecommunications Act 1997* (Cth)

Parliamentary Joint Committee on Intelligence and Security

3 December 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 members of its National Criminal Law Committee in the preparation of this submission.

Executive Summary

1. The Law Council welcomes the opportunity to make this submission to the Committee's review of the Telecommunications Sector Security Regime (**TSSR**) in Part 14 of the *Telecommunications Act 1997* (Cth) (**Telecommunications Act**). This submission focuses on six aspects of the TSSR, and makes recommendations for improvements and further scrutiny. The six matters are as follows:

   (1) interaction of the TSSR with the significant expansion proposed to the *Security of Critical Infrastructure Act 2018* (Cth) (**SCI Act**), as outlined in the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (**ED Bill**), given that the telecommunications sector is proposed to be covered by the expanded regime in the SCI Act;

   (2) two issues relating to the definition of 'security' and the functions of the Australian Security Intelligence Organisation (**ASIO**) under the TSSR:

      (a) the breadth of the definition of 'security', within the meaning of the *Australian Security Intelligence Organisation Act 1979* (Cth) (**ASIO Act**) as the basis for the regulatory obligations, powers and liabilities imposed under the TSSR (and the expanded regulatory obligations and liabilities proposed in relation to the SCI Act); and

      (b) the absence of clear standards and thresholds for the issuance of adverse security assessments (**ASAs**) by ASIO under Part IV of the ASIO Act in relation to a telecommunications provider, for the purpose of the Minister for Home Affairs issuing a direction under the TSSR requiring the provider to act, or refrain from taking action;

   (3) the need for prompt implementation of recommendations of the Committee in its recent report on its statutory review of the mandatory data retention regime in Chapter 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**), especially with respect to prohibitions on the offshore storage of retained data, and the repeal of the 'backdoor' data access permission in section 280 of the Telecommunications Act;

   (4) a lack of information about the application of the Australian Government Regulator Performance Framework to the Department of Home Affairs in its administration of the TSSR (and the SCI Act). Nor have any reasons been provided for any exemptions which may have been given subsequent to the commencement of the TSSR, which would effectively reverse the Government's assurance to the Committee in 2017 that the Regulator Performance Framework **would apply** to the administration of the TSSR;[1]

   (5) overly broad powers of delegation and authorisation under the TSSR, which enable highly significant regulatory powers to be conferred upon the Communications Access Co-Ordinator (**CAC**) (being several officials in the Department of Home Affairs, including persons at the Executive Level 1 and 2 classifications, appointed by the Minister for Home Affairs under section 6R of the TIA Act); and concerns about potential invalidity in the exercise of some of those powers due to an evident administrative error which led to a 14-month delay in the registration (and therefore commencement) of an amendment to the instrument of appointment; and

   (6) inadequate permitted disclosure provisions in Part 14, which do not expressly authorise disclosures for oversight purposes.

[1] PJCIS, *Report on the Review of the Telecommunications and Other Legislation Amendment Bill 2016*, June 2017, 80 at [6.19]. Cf Department of Home Affairs, *Regulator Performance Framework*, https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/campaign-and-reform/regulatory-reform, which appears to indicate that the framework **has not** been applied to the TSSR or the SCI Act.

Interaction of the TSSR with the expanded SCI regime

2. The ED Bill proposes to expand the range of critical infrastructure sectors and assets able to be regulated by the SCI Act, as well as the applicable regulatory obligations. The additional regulatory obligations include:

   - specific cyber security obligations in relation to private owners and operators of critical infrastructure assets that are deemed in Ministerial rules to be, or form part of, a 'system of national significance'; and

   - a Ministerial authorisation (**MA**) regime enabling the Secretary of the Department of Home Affairs **(Department**) to require the Australian Signals Directorate (**ASD**) to intervene in a cyber security incident occurring (or which has occurred) in relation to a critical infrastructure asset. ASD would be conferred with a comprehensive statutory immunity from any civil or criminal liability for causing loss, damage, interference or obstruction, in respect of acts done in compliance, **or purported compliance**, with a request made by the Secretary under an MA issued by the Home Affairs Minister.

3. Significantly, the ED Bill proposes that the telecommunications sector will be able to be regulated by the expanded regime in the SCI Act,[2] in addition to its existing obligations and liabilities under the TSSR.

Potential duplication, conflict and overlap of regulation

4. The Law Council acknowledges that there is a policy intent to avoid duplication, including awaiting the outcomes of the Committee's present review of the TSSR before setting the content of security obligations under an expanded SCI regime (if such legislation is introduced and passed before the Committee reports on TSSR).[3]

5. The ED Bill also proposes to delegate legislative powers to the Minister to make rules excluding certain telecommunications assets from the operation of the SCI regime. It would also be open to the Minister to make rules prescribing the substance of regulatory obligations for the communications sector under the SCI Act as simply the fulfilment of existing obligations under the TSSR.[4]

6. However, this means that any avoidance of regulatory duplication or oppression as a result of exposure to multiple regulatory obligations is left almost entirely to executive discretion. Moreover, no draft rules for the communications sector (or any other sector) were released with the ED Bill that could offer any tangible assurance about the intended exercise of delegated legislative powers.

Increased regulatory burden

7. In any event, the telecommunications sector will be subject to additional regulatory obligations to those under the TSSR, even if the delegated legislative powers proposed under the SCI Act are exercised in the manner suggested. This includes:

[2] ED Bill, Schedule 1, item 7 (amending section 5 of the SCI Act to insert the definition of 'critical telecommunications asset'); and item 21 (inserting sections 8D and 8E of the SCI Act, to create definitions of 'critical infrastructure sector,' which includes '(a) the communications sector'; and 'critical infrastructure asset', which provides that a 'critical telecommunications asset' is taken to relate to the communications sector').

[3] Department of Home Affairs, *Explanatory Document to the ED Bill*, (November 2020), 8 at [40]; 12 at [60].

[4] ED Bill, Schedule 1, items 22-29 (amendments to section 9 of the SCI Act); and items 39 and 45 (inserting the new security obligations, including delegated legislative powers to prescribe the contents of rules or other regulatory obligations for individual critical infrastructure sectors or assets).

- liability to two sets of Ministerial direction powers to do, or omit to do, certain things on security related grounds (one under the TSSR and the other under the existing provisions of the SCI Act);

- potential liability to additional cyber security obligations, including incident notification and planning, and liability to government intervention in cyber incidents affecting telecommunications infrastructure; and

- liability to two sets of enforcement powers, one under the Telecommunications Act (including as conditions of carrier licences, or requirements under statutory rules applicable to carriage service providers), and the other under the SCI Act. The proposed enforcement powers under the SCI Act will include the potential exercise by the Department of Home Affairs of highly intrusive powers of monitoring and investigation that are not available under the TSSR. This includes the power to enter private premises, and secure (by making non-operational) and seize items on those premises.

Incompatibilities between TSSR and expanded SCI regime

8. In addition to the management of risks of duplication or oppression being left substantially to executive discretion, the Law Council has also identified several inconsistencies. They include:

- ***secrecy obligations:*** the SCI regime is subject to highly restrictive secrecy obligations in sections 45-47 of the SCI Act, which do not clearly permit disclosures for the purpose of oversight or obtaining legal advice. Section 47 of the SCI Act further purports to override the information-gathering powers of courts, tribunals and oversight agencies such as the Commonwealth Ombudsman. No such restrictions apply under the TSSR;

- ***officials with regulatory responsibilities:*** under the TSSR, most regulatory and administrative responsibilities are performed by the CAC (being a person or persons who are appointed by the Minister for Home Affairs under section 6R of the TIA Act). Presently, numerous staff of the Department of Home Affairs are appointed to the position, including all staff at the Executive Level 1 and 2 classifications in specified organisational units within the Department.[5] In contrast, the equivalent regulatory functions proposed under the SCI Act in the ED Bill are conferred on the Secretary, and are delegable only to employees of the Department holding positions classified as Senior Executive Service (**SES**) levels.[6] This is a very significant difference in the seniority of persons who may be authorised to perform the same or substantially similar regulatory functions;

- ***compulsory information-gathering powers***: under the TSSR, the Secretary of the Department of Home Affairs may delegate their information-gathering powers to the Director-General of Security (and only the Director-General).[7] In contrast, the ED Bill proposes that the Secretary's information-gathering powers under the SCI Act (under the expanded regime) will be delegable to any SES-level employee of the Department.[8] Accordingly, there is very significant variation in the levels of seniority and expertise of the persons who may be able to exercise the same, or substantially similar, intrusive powers to obtain, use and disclose sensitive information (potentially including the confidential commercial information of telecommunications providers); and

[5] Telecommunications (Interception and Access) (Communications Access Co-ordinator) Instrument 2019.

[6] SCI Act, section 59.

[7] Telecommunications Act, section 315G.

[8] SCI Act, section 59.

- ***enforcement bodies:*** many breaches of regulatory obligations under the TSSR will be enforceable by the Australian Communications and Media Authority (**ACMA**) under carriers' licence conditions and conditions of statutory rules for carriage service providers under the Telecommunications Act.[9] In contrast, the SCI Act contains a dedicated civil penalty and enforcement regime, which is proposed to be expanded significantly by the ED Bill. The Secretary of the Department of Home Affairs (or delegate) would be the 'authorised applicant' for the enforcement powers under the SCI Act, unless the Secretary has, at their discretion, appointed the head and senior staff of another Commonwealth regulatory body (such as the CEO and SES-level staff of the ACMA).[10] It is therefore possible that there will be differences in exposure to liability and penalty, and differences in regulatory approaches under the TSSR and SCI regime.

Recommendation 1—harmonisation of the proposed SCI Act expansions with TSSR

- **The proposed expansions to the regulatory regime in the SCI Act should not be passed unless and until the Committee has had an adequate opportunity to undertake a comprehensive review of both the relevant amending Bill (when introduced) and the TSSR, including with a view to addressing the concerns raised at paragraphs [4]-[8] of this submission.**

Other Law Council concerns about the expanded SCI regime (see Attachment 1)

9. More broadly, in its submission to the Department on the ED Bill, the Law Council raised a number of concerns about the proposed expansion of the SCI regime. These concerns focused particularly on the proposed MA regime, and arrangements for independent oversight and review (both judicial review and merits review).

10. As these matters are relevant to the regulatory impost of the TSSR and expanded SCI regime on telecommunications carriers, carriage service providers and intermediaries, a copy of the Law Council's submission on the ED Bill is provided as **Attachment 1** to this submission.[11]

Adoption of the definition of 'security' in the ASIO Act

11. The term 'security', as defined in section 4 of the ASIO Act, is the central concept for the application of the major regulatory powers, obligations and liabilities in the TSSR.

12. The protection of security is the central purpose for which telecommunications carriers, carriage service providers and intermediaries must comply with their regulatory obligations under section 313 to do their best to protect their networks and assets; and their obligations under Division 3 of Part 14 to periodically lodge security capability plans and make notifications of changes to their networks.

13. The concept of 'security' as defined in the ASIO Act is also central to the exercise by the Minister for Home Affairs of the power to issue binding directions under sections

[9] Telecommunications Act, sections 61, 68, 98 and 101 and Schedules 1 and 2 (standard carrier licence conditions and carriage service provider rules) which include obligations to comply with the requirements of the Telecommunications Act.

[10] ED Bill, Schedule 1, item 56 (amending section 49 of the SCI Act).

[11] The Law Council's submission to the Department of Home Affairs on the ED Bill is also published at: https://www.lawcouncil.asn.au/resources/submissions/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020.

315A and 315B, requiring a telecommunications entity to do, or refrain from doing, a specified act or acts on security-related grounds.

14. In addition, Commonwealth officials are empowered to use and disclose information obtained from telecommunications providers under the TSSR (including confidential, commercially sensitive information) for the purposes of 'security' within the meaning of the ASIO Act.

15. As the Law Council has observed previously, the concept of security in section 4 of the ASIO Act extends far beyond the ordinary meaning of that term, and is overly broad for the purpose of the more significant regulatory obligations imposed under the TSSR. The Law Council is also concerned that this overbreadth would be exacerbated if the proposals identified in the submission of the Department of Home Affairs to the present inquiry are adopted, to amend the general security obligation in section 313 to be more prescriptive of the actions that carriers, carriage service providers and intermediaries must take to protect their networks and assets from being used for activities prejudicial to security.

16. Under section 4 of the ASIO Act, the term 'security; covers:

    (a) espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, and acts of foreign interference;

    (aa) the protection of Australia's territorial and border integrity from serious threats; and

    (b) the carrying out of Australia's obligations to any foreign country in respect of the matters in paragraphs (a) and (aa) above.

17. In addition to the breadth of each component term in the concept of 'security' in the ASIO Act, the Law Council also notes that:

    - extending the TSSR to cover the matter in paragraph (b) (**Australia's obligations to other countries**) has not been demonstrated to be necessary or proportionate to a legitimate objective in respect of securing Australia's telecommunications systems. The Law Council continues to support the exclusion from the TSSR of paragraph (b) of the ASIO Act definition;

    - the component term **'politically motivated violence'** (also defined in section 4 of the ASIO Act) is technically capable of covering legitimate protest and dissent, including the actions of people who do not personally engage in violence, but their protest or advocacy may attract 'counter-protestors' who may engage in violence. However, separate statutory limitations in section 17A of the ASIO Act and the Minister's Guidelines to ASIO (made under section 8A of that Act) attempt to limit that ASIO's investigative activities in relation to such legitimate activity. No such limitations are imported into the TSSR. The Law Council considers that specific limitations are required; and

    - the component term **'acts of foreign interference'** (also defined in section 4 of the ASIO Act) is not limited to acts that are done by, or at the behest of, a foreign power, which are clandestine and deceptive and are carried on for intelligence purposes. They also include acts that are carried on for the purpose of affecting political or governmental processes (which could potentially cover good faith policy advocacy) and acts which are, in any way, detrimental to Australia's interests (as may be determined or interpreted by those administering the TSSR from time-to-time, without any specification as to the requisite degree of detriment). In contrast to the requirements in the Minister's Guidelines to ASIO made under section 8A of the ASIO Act, which

prescribe various approval requirements and proportionality thresholds for the conduct of intelligence collection investigations and exercise of powers by ASIO, no equivalent limitations are imported into the TSSR. The broad concept of 'acts of foreign interference' is therefore 'at large' in the TSSR.

18. The Law Council acknowledges that there is a legitimate interest in the Government working collaboratively with the telecommunications sector in relation to all risks within the definition of security in the ASIO Act. However, for the imposition of **significant, legally binding regulatory obligations and liabilities** under the TSSR to be reasonably regarded as being proportionate to a legitimate security-related objective, greater precision in the scope of the operative concept of 'security' (and its component terms) is necessary.

19. Presently, for example, a telecommunications carrier is potentially exposed to the loss of their carrier licence if they fail to comply with obligations purported to be imposed under the TSSR (including Ministerial directions) that are directed to:

- fulfilling any obligations Australia may have to foreign governments, which are covered by paragraph (b) of the definition of security. Such obligations to foreign governments may arise under bilateral agreements which are in force from time-to-time, the details of which may be kept secret for any reason; and
- preventing telecommunications carrier from providing services to a company that is owned or controlled (in full or in part) by a business enterprise of a foreign government, which may be engaging in legitimate policy advocacy about regulatory matters affecting the conduct of that business. (Noting that there is scope for argument that this activity by the foreign business enterprise is caught by the definition of 'acts of foreign interference' as a component of the definition of 'security' in the ASIO Act).

Recommendation 2—use of the ASIO Act definition of security

- **The definition of security for the purpose of Part 14 of the Telecommunications Act should be amended so that:**
  - **the matters covered by paragraph (b) of the definition of security in section 4 of the ASIO Act are not within the scope of 'security' under the TSSR; and**
  - **there are specific protections for activities involving legitimate protest and dissent, to ensure that these activities do not trigger the application of the TSSR, as a form of 'politically motivated violence' within the ASIO Act definition of security (noting that the protections found in section 17A of the ASIO Act and the ASIO Guidelines do not apply to the TSSR).**

Threshold for furnishing ASAs in relation to the TSSR

20. The Law Council supports the retention of the issuance of a merits reviewable ASA as a precondition to the Home Affairs Minister exercising a power of direction under sections 315A and 315B of the Telecommunications Act (and the corresponding power of direction under section 32 of the SCI Act).

21. However, as the Law Council has commented previously, the thresholds for issuing an ASA under Part IV of the ASIO Act are opaque. This is particularly problematic in the context of Australia's domestic regulatory regimes in relation to critical infrastructure, on which millions of Australians and the national economy rely and could be significantly affected by directions issued to their providers under the TSSR (or SCI Act, or both regimes if the proposed amendments are enacted).

22. An ASA is defined in section 35 of the ASIO Act as a security assessment in respect of a person (including a company) that contains:

    (a) any opinion or advice, or any qualification of any opinion or advice, or any information that is or could be prejudicial to the interests of the person; and

    (b) a recommendation that prescribed administrative action be taken or not taken in respect of the person, being a recommendation the implementation of which would be prejudicial to the interests of the person.

23. The issuing of an ASA is not required to be based on conventional standards of proof, such as the civil standard of the balance or probabilities. The specific criteria by which ASIO makes its assessments are also largely unknown. While merits review will be available in the Security Division of the Administrative Appeals Tribunal (which the Law Council welcomes) that will not necessarily disclose to regulated entities the criteria used in the issuance of the ASA, and thereby allow them to proactively structure their business activities in a manner that avoids their being made subject to an ASA and consequent Ministerial direction under the TSSR.

24. If ASAs are to be used in domestic regulatory regimes such as the TSSR (and the regime under the SCI Act, particularly if expanded to the communications sector in addition to the TSSR), then there should be increased transparency.

25. More generally, the Law Council notes that, despite the increased reliance that major regulatory regimes such as the TSSR and SCI Act are placing on the security assessment regime, Part IV of the ASIO Act is the sole major part of the ASIO Act that has not been subject to detailed review and potential modernisation-type reforms. Most other parts of the ASIO Act (including special powers warrants) were reviewed by the PJCIS in 2012 and 2013[12] and were subsequently amended in 2014.[13] The Law Council considers that the security assessment regime requires review to ensure that it remains fit-for-purpose in contemporary circumstances.

26. Given the expanded use of the security assessment regime, this should include consideration of interests in transparency, procedural fairness and accessibility of review rights.

27. As a related matter, if such a review of Part IV is to be undertaken, the Law Council considers that it should also specifically consider the legal rights of people who are the subject of security assessments by ASIO, but there are prolonged delays in ASIO's completion of that assessment (in the nature of many months or years).

28. The Law Council notes that merits review rights only apply to ASIO's decisions to furnish ASAs. There are no apparent statutory rights available where there is a failure by ASIO to complete a security assessment within a certain time, including in cases in which a non-prejudicial security assessment is a condition precedent to an administrative decision for the conferral of a benefit on the person (such as a security clearance or a visa, for the purposes of a person's employment, residence or study in Australia).The Law Council is concerned that this is a gap in the rights available to people who are subject to security assessments. The more use that is made of security assessments in administrative and regulatory regimes, the greater the potential for this gap to have serious, detrimental impacts.

[12] PJCIS, *Report on Inquiry into Proposed Reforms of National Security Legislation*, (June 2013).

[13] *National Security Legislation Amendment Act (No 1) 2014* (Cth). See further: PJCIS, *Report on Review of the National Security Legislation Amendment Bill (No 1) 2014*, (September 2014).

Recommendation 3—Adverse Security Assessments in connection with TSSR

- **If ASAs are to be used as the basis for issuing Ministerial directions under the TSSR and SCI Act, they should be subject to greater transparency requirements, in relation to the assessment criteria and the threshold for issuance (such as applying the civil standard of proof).**
- **More broadly, the security assessment provisions of Part IV of the ASIO Act require independent review and potential modernisation, including with a view to improving transparency, procedural fairness, the accessibility of merits review rights with respect to ASAs, and providing for the rights of the subjects of security assessments where there are protracted delays by ASIO in completing those assessments.**

Recommendations from the data retention review

29. The Law Council supports the timely implementation of recommendations of the Committee in its recent statutory review of the data retention regime in the TIA Act, all of which are relevant to the operation of the TSSR.[14] This reflects that telecommunications carriers and carriage service providers are subject to security obligations under the TSSR in respect of the telecommunications data which they are required to retain under the TIA Act.

30. The Committee's data retention recommendations that are of particular relevance to the TSSR include the following:

    - a prohibition on the storage of retained data outside Australia, unless an entity is specifically exempt;[15] and
    - stronger protections in respect of disclosures of retained data, in respect of which telecommunications carriers and carriage service providers are subject to the TSSR obligations. In particular, it recommended the repeal of paragraph 280(1)(b) of the Telecommunications Act, which enables the disclosure of telecommunications data outside the limited recipients prescribed in the TIA Act, provided that another Commonwealth, State or Territory law purports to authorise access.[16]

31. At the time of writing this submission, a Government response to the Committee's report remained outstanding. The Law Council urges the Government to adopt, and implement promptly, all of the Committee's recommendations in its review of the mandatory data retention regime.

32. The Law Council considers that the Parliament should not countenance any proposed expansions of the SCI regime (including in relation to the telecommunications sector, which is presently already regulated by the TSSR), or any amendments to the TSSR regime, until the Committee's recommendations on data retention are implemented fully.

Recommendation 4—outstanding recommendations of data retention review

- **The Committee should not recommend passage of any proposed expansions of the SCI Act (which the Law Council understands are to be introduced in December 2020) or the TSSR unless and until the**

[14] PJCIS, *Report on the Review of the Mandatory Data Retention Regime*, (October 2020).
[15] Ibid, 123-124 at [5.120]-[5.124] and recommendation 21.
[16] Ibid, 118-119 at [5.97]-[5.99] and recommendation 15.

Government has:

- **accepted the Committee's recommendations in its review of the mandatory data retention regime; and**
- **has introduced legislative amendments (potentially as part of the SCI amendments) to implement recommendations 15 and 21 of the Committee's review of the mandatory data retention regime.**

Application of the Regulator Performance Framework

33. During the Committee's review of the originating Bill to the TSSR in 2016-17, the (then) responsible portfolio department, the Attorney-General's Department, provided the Committee with an assurance that the administration of the new regime would be subject to the Australian Government Regulator Performance Framework.[17] The Committee sought this assurance because stakeholders participating in the inquiry expressed support for the application of that framework, and raised concerns that no formal commitment had been made in this regard.[18]

34. While the Committee recommended that a range of regulatory performance measures be included in the separate annual reports that are required to be prepared and tabled under section 315J, this recommendation appeared to be **in addition to** the Committee's understanding that the reporting requirements under the Regulator Performance Framework would apply.[19] That is, there would also be annual evaluations of, and public reporting against, the following key performance indicators (**KPIs**) prescribed by the Regulator Performance Framework:

    - regulators do not unnecessarily impede the efficient operation of regulated entities;
    - communication with regulated entities is clear, targeted and effective;
    - actions undertaken by regulators are proportionate to the risk being managed;
    - compliance and monitoring approaches are streamlined and coordinated;
    - regulators are open and transparent in their dealings with regulated entities; and
    - regulators actively contribute to the continuous improvement of regulatory frameworks.

35. The Law Council notes that the annual reports on the operation of the TSSR, which are prepared under section 315J of the Telecommunications Act, do not appear to include sections reporting specifically against the KPIs in the Regulator Performance Framework.[20] The Department's webpage on TSSR also does not appear to make reference to the application of the Regulator Performance Framework.

[17] PJCIS, *Report on the Review of the Telecommunications and Other Legislation Amendment Bill 2016*, June 2017, 76 at [6.3] (including footnote 5, which cited the relevant evidence of the Attorney-General's Department to the Committee on 23 March 2017) and 80 at [6.19].

[18] Ibid, 75-76 at [6.2]-[6.4].

[19] Ibid, 80-81, recommendation 7.

[20] See, for example, Department of Home Affairs, *Telecommunications Sector Security Reforms: 2019-20 Annual Report*, (Undated, 2020).

36. Further, there do not appear to be separate Regulator Performance Framework reports published on the part of the Department's website dealing with its compliance with that framework in relation to its administration of TSSR.[21]

37. In fact, the Department's website states that the Regulator Performance Framework applies only to limited aspects of the Department's activities, which do not include the TSSR or SCI regime (namely, migration, aviation and maritime security, and border-related matters affecting trade, travel and customs). The Department's annual regulatory performance reports therefore do not address its functions under the TSSR and SCI regime.

38. The Law Council would be concerned if there has been an unannounced decision to retreat from the Government's statement of commitment to the Committee in 2017 that the Regulator Performance Framework would apply to the operation of the TSSR. The Law Council therefore recommends that the Committee seeks an assurance from the Department about this matter, which could include seeking detailed information about:

- how the Regulator Performance Framework is applied in the Department's regulatory planning process, and in its regulatory operations under the TSSR;
- how the Department's performance under the Regulator Performance Framework in relation to the TSSR is specifically evaluated (including whether any feedback is sought and obtained from regulated entities), and details of its reporting (including frequency of reports, to whom they are provided, and whether they are made available publicly); and
- if the Government or the Department has decided to exclude the TSSR from the Regulator Performance Framework:
  - an explanation of the reasons for this decision; and
  - a further explanation of the reasons that the public (including industry and civil society stakeholders) were not consulted on, or informed of, that decision, in view of the fact that the Committee specifically sought and obtained an assurance from the Government in 2017 as a result of stakeholder concerns raised during the review of the Bill.

39. The Law Council considers that the Department's administration of the TSSR and SCI Act should be subject to the Regulator Performance Framework. Evaluation reports should be made public and uploaded to the Department's Regulator Performance Framework webpage.

40. This reflects the critical need for regulated entities, the Parliament and the wider community to have a credible basis upon which to be assured of the Department's competence and performance as a regulator under the TSSR. Such a regime is not a matter that typically falls within the normal expertise of a department whose primary function is (apart from the functions of the Australian Border Force) the provision of policy advice and program administration support to the Government. A high degree of transparency is needed.

41. The inclusion of the TSSR and SCI regime in the Regulator Performance Framework is even more important given the proposed expansion of the SCI regime, which will cover the telecommunications sector and will expose all regulated entities under the SCI Act to significant additional obligations and liabilities.

[21] Department of Home Affairs, *Regulator Performance Framework*, https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/campaign-and-reform/regulatory-reform.

Recommendation 5—application of the Regulator Performance Framework

- **The Department of Home Affairs should be subject to the Australian Government Regulator Performance Requirement in relation to the TSSR (and SCI Act).**
- **The Government should provide a public explanation of why the assurance provided to the Committee in 2017 that the TSSR would be subject to the Regulator Performance Framework does not appear to have been honoured, given the absence of any reference to the TSSR on the Department's Regulator Performance Framework webpage.**

Powers of delegation and authorisation

The Communications Access Co-Ordinator

42. The CAC is conferred with numerous regulatory functions and powers under the TSSR. This includes:

- making determinations that certain network or other changes do not need to be notified under section 314A, and exempting individual carriers or providers from notification obligations under that section;
- conducting assessments of, and providing advice on, the security implications of proposed network or other changes under section 314B; and
- conducting assessments of, and providing advice on, carriers' and providers' security capability plans under section 314D.

43. As noted above, the CAC is appointed by the Minister for Home Affairs by legislative instrument made under section 6R of the TIA Act. Presently, several employees of the Department of Home Affairs are appointed to the role.[22] As the appointments are made by reference to all persons who hold positions of a particular classification in various administrative areas of the Department, and there may be multiple such positions, it is not possible to know:

- the total number of persons who are appointed as CAC;
- of those appointees, the persons who, in fact, perform functions and exercise powers as CAC specifically in relation to the TSSR; and
- the governance arrangements within the Department for the performance of functions and exercise of powers by persons appointed as CAC. (The Law Council envisages that such governance arrangements would cover matters including training and continuing education; substantive and perceived independence; conflict of interest management and other arrangements with respect to probity; mechanisms for the allocation of responsibilities and de-confliction among multiple appointees; assurance and oversight programs; regulatory performance evaluation; and internal review arrangements in relation to the administrative decisions of persons appointed as CAC.)

44. In addition, some of the positions appointed as CAC under the current instrument of appointment appear to be of a disproportionately low level of seniority, relative to the significant of the regulatory powers invested in the CAC. For example, persons holding positions (including on an acting basis) classified as Executive Level 1 are appointed as CAC. The appointment of persons at this level to perform significant

[22] Telecommunications (Interception and Access) (Communications Access Co-ordinator) Instrument 2019.

regulatory functions, which may trigger significant compliance costs and exposure to legal liability for regulated entities, raises questions about whether it is realistic to expect that such appointees would be capable, both in substance and perception, of acting without external influence or a significant risk of such influence. (That is, there is a risk that such officers may effectively 'act under dictation' by more senior Departmental officials, including those officials to whom they directly or indirectly report in performing their ordinary duties of employment.)

45. Further, irrespective of the level of seniority of individual appointees to the role of CAC, it is not clear, on the basis of all of the named administrative areas in the instrument of appointment, that all of the persons who are appointed as CAC (and are therefore legally capable of exercising powers under the TSSR) would necessarily have the specific technical and regulatory skills to effectively perform the substantive regulatory functions and powers conferred on the CAC, including under the TSSR.

46. While the position of the CAC was originally established to coordinate information obtained or sought under the TIA Act, it has increasingly been conferred with substantive regulatory powers and functions under multiple, unrelated pieces of security legislation. This includes under the data retention regime in the TIA Act, enforcement powers in relation to the compulsory industry assistance regime in Part 15 of the Telecommunications Act, and proposed enforcement powers in the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 presently under review by the Committee.

47. In contrast, the Law Council notes that, under the proposed expansions to the SCI Act, the Secretary would perform the relevant functions and could only delegate their powers to SES-level employees of the Department.

48. The Law Council is further concerned that there was recently an approximately 14-month delay in registering a legislative instrument making changes to the appointment of persons as CAC, to reflect an organisational restructure of the Department.[23] This appears to have been an administrative error. However, it may call into question the validity of acts done by persons purporting to act as CAC for that period of delay.

49. The Law Council considers that, in combination, these circumstances merit a re-thinking of whether the CAC is the most appropriate entity to perform the regulatory functions under the TSSR (or under other legislation) and, if so, whether:

[23] See: Telecommunications (Interception and Access) (Communications Access Co Ordinator) Instrument 2019 (made 1 July 2019 and registered 7 September 2020) (**2019 instrument of appointment**).

The 2019 instrument of appointment was registered one day before a further amending instrument, the Telecommunications (Interception and Access) (Communications Access Co Ordinator) Amendment Instrument 2020 (made and registered 8 September 2020) (**2020 amending instrument**). It appears to the Law Council that the failure to register the 2019 instrument of appointment was identified when the 2020 amending instrument was being prepared.

However, the delayed registration (and therefore commencement) of the 2019 instrument of appointment call into question the validity of acts done in purported reliance on that instrument, from 2 July 2019 to 7 September 2020, as the previous instrument—the Telecommunications (Interception and Access) (Communications Access Co-ordinator) Instrument 2018 (**2018 instrument**)—would have been in force for that period. The 2018 instrument would have appointed persons by reference to positions within the Department that no longer existed because of its restructure. This means that the class of persons appointed may not have been capable of being identified with sufficient specificity in order for the 2018 instrument to be valid beyond the Departmental restructure.

As the explanatory statements to the 2019 instrument of appointment and the 2020 amending instrument did not acknowledge or explain the reasons for the delayed registration of the 2019 instrument, it is unknown whether any powers or functions were purportedly exercised by Departmental staff between 2 July 2019 and 7 September 2020, and if so, which functions or powers may now be in doubt (including in relation to the TSSR).

- section 6R of the TIA Act should be amended to insert statutory criteria for the appointment of persons as CAC, to prescribe minimum levels of seniority and expertise for appointment (at least with respect to particular regulatory powers and functions);

- there are adequate oversight, reporting and other transparency measures in relation to the exercise of powers by persons appointed as CAC; and

- the Department has implemented adequate assurance mechanisms in respect of the making and registration of instruments of appointment, to:

  - avoid repetition of the recent, prolonged delay in registering key updates to appointments; and

  - identify any remedial action that may be needed to validate acts done in purported reliance on amendments to the instrument of appointment, during the prolonged period of delay (of over 12 months) in the registration of that instrument.[24]

50. The Law Council's preference is that powers are invested in the Secretary of the Department, with a limited power of delegation to SES-level staff who, in the opinion of the Secretary based on reasonable grounds, have appropriate technical and regulatory expertise to perform the relevant functions.

Recommendation 6—functions of the Communications Access Co-Ordinator

- **Part 14 of the Telecommunications Act should be amended to:**
  - **repeal provisions conferring regulatory powers and functions on the CAC; and**
  - **substitute these provisions with equivalent powers of authorisation and delegation to those in the SCI Act (namely, the powers and functions should be conferred on the Secretary subject to a power of delegation in favour of SES-level employees of the Department).**
- **The Government, via the Department, should provide an explanation to the Committee and wider public of the matters noted at paragraph [49] of this submission, regarding the 14-month delay in the registration of an instrument of appointment of certain officials as CAC under section 6R of the TIA Act.**

Secretary's power to delegate information-gathering powers

51. Section 315G authorises the Secretary to delegate their information-gathering powers under the TSSR to the Director-General of Security (to the exclusion of any Departmental staff). As noted above, this contrasts with the powers of delegation proposed in the expansions to the SCI regime, which are limited to Departmental SES-level employees.

52. In addition to recommending harmonisation of the power of delegation (noting the proposal for both the TSSR and SCI Act to apply to telecommunications carriers, carriage service providers and intermediaries) the Law Council suggests that the Committee seeks further information about the exercise of the power of delegation

[24] The Law Council understands that the Senate Committee for the Scrutiny of Delegated Legislation is presently considering these issues, and has written to the Minister for Home Affairs seeking further information: Senate Standing Committee for the Scrutiny of Delegated Legislation, *Delegated Legislation Monitor 12 of 2020,* (November 2020), 21 (see also the letter to the Minister dated 12 November 2020).

under section 315G. In particular, the Committee may wish to seek information from the Department as to:

- whether the power has been delegated to the Director-General of Security;
- if so, whether the delegation was made subject to directions about the exercise of the delegated power (and the contents of any such directions); and
- whether the delegated power has been:
  - exercised by the Director-General of Security; and
  - contemplated but ultimately not exercised, in favour of other powers to obtain information (including the use of the power to confer civil immunities under section 21A of the ASIO Act, or the exercise by ASIO of its covert powers under warrant or authorisation).

53. On the latter point, the Law Council also notes that, given the subsequent enactment of section 21A of the ASIO Act in 2018 (which enables ASIO to request information from any person, in exchange for the conferral of a civil immunity), the power of delegation to the Director-General in section 315G of the Telecommunications Act may be otiose. In any case, there is now extensive duplication, which raises propriety risks in decision-making about, and the exercise of, each set of information-gathering powers.

54. More generally, the conferral of a power on one agency head to delegate their powers to the head of another agency (with their own statutory functions, obligations and interests in relation their own agency's activities) may raise particular challenges and risks in relation to the effective governance of that power. The fact that ASIO is exempt from the Privacy Act, whereas the Department of Home Affairs is not, may also have implications for the treatment of information obtained from telecommunications providers under any exercise of the delegated information-gathering power pursuant to section 315G.

Recommendation 7—Secretary's power of delegation to DG Security

- **Section 315G of the Telecommunications Act should be amended to omit the Secretary's power of delegation to the Director-General of Security, and substitute this with a power of delegation to SES-level Departmental employees, consistent with the powers of delegation in the SCI Act.**
- **The Department should provide to the Committee the information about the matters referred to at paragraph [52] of this submission, regarding the exercise of the existing power of delegation in section 315G.**

Absence of permitted disclosures for oversight purposes

55. Section 315H of the Telecommunications Act permits the disclosure of information obtained in the exercise of compulsory information-gathering powers under Part 14 for the purposes of assessing risks to networks or facilities, or otherwise for the purposes of security (as that term is defined in section 4 of the ASIO Act).

56. The Law Council is concerned that there is no explicit direction in relation to disclosures made for the purpose of independent oversight of the operation of Part 14. While section 315H does not directly impose an offence, it can operate in combination with the official secrecy offences in Part 5.6 of the *Criminal Code Act 1995* (Cth).

57. It would therefore be preferable for it to be made explicit, **on the face of Part 14**, that it is lawful and proper to disclose information obtained under that Part to an independent oversight body, for the purpose of that body performing functions or duties of exercising powers.

58. Given the broad secondary uses that are permitted under subsection 315H(1), in combination with the definition of 'Commonwealth officer' in subsection 315H(4), the amendments recommended by the Law Council should expressly permit disclosures to the Commonwealth Ombudsman, Australian Information Commissioner, Inspector-General of Intelligence and Security, Australian Law Enforcement Integrity Commissioner and Inspector-General of the Australian Defence Force.

Recommendation 8—permitted disclosures for oversight purposes

- **Section 315H of the Telecommunications Act should be amended to include an explicit 'permitted disclosure' provision enabling all information obtained under Part 14 to be disclosed to independent oversight bodies with functions in relation to TSSR. As a minimum, this should include the bodies specified at paragraph [58] of this submission.**

Further statutory review and oversight of the TSSR

59. The Law Council's submission to the Department on the ED Bill (**see Attachment 1**) made several recommendations to enhance review and oversight of the expanded SCI regime, which the Law Council considers should apply equally to the TSSR. These include the following measures:

- further statutory reviews by the Committee. (This could be accompanied by any modernisation type amendments to the Committee's governing legislation, which the Committee may consider necessary or desirable to facilitate its legislative scrutiny and review activities—for example, more flexible provisions enabling the use of sub-committees);

- the conferral of an inspection function on the Commonwealth Ombudsman (and a commensurate increase in funding for that office, including to enable the acquisition of security-related infrastructure and security cleared personnel as required, and access to independent technical expertise); and

- the Government or the Parliament (or both) nominating a performance audit priority to the Commonwealth Auditor-General, being the administration by the Home Affairs portfolio of the SCI regime and the TSSR. Resourcing for the Australian National Audit Office should be increased, including to enable performance auditing of the implementation of major recent expansions to national security legislation. (Independent performance auditing will be particularly important for measures with significant regulatory impacts on the private sector, or which otherwise involve the performance by the Department of Home Affairs of regulatory functions.)

Recommendation 9—further statutory review and oversight of the TSSR

- **Part 14 of the Telecommunications Act should be amended to make provision for the periodic statutory review, and standing inspection functions of the Commonwealth Ombudsman set out at paragraph [59] of this submission, consistent with the Law Council's submission on the ED Bill proposing to amend the SCI Act.**
- **The Committee should consider writing to the Commonwealth Auditor-General nominating the regulatory and administrative functions of the**

Department of Home Affairs in relation to the TSSR and SCI Act as a performance audit priority. The Law Council recommends that the Government should support such an audit priority, as a tangible demonstration of its commitment to an effective (and continuously improving) regulatory framework for the security of privately held critical infrastructure assets, including the telecommunications sector.

- **The Government should increase the budget of the Australian National Audit Office to conduct further performance audits, including of the regulatory and administrative activities of the Home Affairs portfolio in relation to major recent expansions of national security legislation (including TSSR and the SCI Act).**