Law Council
OF AUSTRALIA

Exposure Draft:

Security Legislation Amendment (Critical Infrastructure) Bill 2020

Department of Home Affairs

27 November 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.

Acknowledgements

Law Council contributors

The Law Council gratefully acknowledges the contributions of the Business Law Section to this submission.

Consultative process

The Law Council commends the Department of Home Affairs (**Department**) for releasing exposure draft legislation prior to the anticipated introduction of a Bill to Parliament in the final sitting fortnight of 2020 (commencing 30 November).

The release of an exposure draft Bill was supported by the Law Council and other stakeholders who made submissions on the previous consultation paper, *Protecting Critical Infrastructure and Systems of National Significance,* during the eight-week consultation period in August-September 2020.

The Law Council also welcomes the Government's statement of commitment in the explanatory document accompanying the exposure draft legislation, which undertakes to adopt the principles of partnership and co-design in the development and administration of the expanded regulatory framework for critical infrastructure security, particularly with respect to cyber security capability and incident responses.

However, as noted in this submission, the Law Council is concerned by the limited time allocated for consultation relative to the significance of the proposals; and the conduct of separate and consecutive consultation processes on critical infrastructure and foreign investment measures despite their interaction.

Nonetheless, the efforts made to consult stakeholders on this package of regulatory changes, prior to the introduction of legislation, are appreciated. The Law Council would welcome the adoption of such consultation for other proposed amendments to national security and criminal legislation, particularly proposals to confer extraordinary powers on security and law enforcement agencies, or to depart significantly from established principles of criminal law.

Executive Summary

1. The Law Council of Australia welcomes the opportunity to comment on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill (**ED Bill**).

2. The Law Council supports the objective of the Bill to create a transparent and coordinated national regulatory framework for the security of critical infrastructure, which focuses on building resilience against attack or compromise. The Law Council acknowledges the regulatory focus on cyber security, which reflects the major dependence on electronic communications and transactions across all sectors of the Australian economy and society, in all facets of business and personal life.

3. The Law Council welcomes the stated intent to ensure that the regulatory burden of the new regime is no greater than is necessary and proportionate to achieve this legitimate policy objective. The explanatory materials indicate that the Government is alert to the need to avoid duplication of existing sector-specific regulation; and to take a measured and risk-based approach to enforcement and government intervention in responding to cyber security incidents affecting private infrastructure.

4. The Law Council's aim is to ensure that these objectives are given full expression in the legislative framework. It is critical that the primary legislation contains adequate safeguards, which **require** the scheme to operate in a targeted, proportionate, fair and accountable way, rather than being overly reliant on executive discretion.

5. The Law Council raises two overarching issues, summarised below, in respect of which several amendments are recommended in this submission. The Law Council also cautions against seeking the urgent passage of this legislation in the remaining eight Parliamentary sitting days of 2020, given its complexity and potential impacts.

Delegations of legislative power

6. The ED Bill proposes broad delegations of legislative power, both to prescribe the scope and coverage of regulatory obligations, and the nature of government intervention in responding to cyber security incidents affecting private infrastructure.

7. While appreciating the need for flexibility to tailor requirements to individual sectors, and to respond urgently to cyber security incidents, the Law Council considers that the proposed delegations of legislative power require stronger statutory parameters on their scope and manner of exercise. The Law Council also considers that the Parliament should have a stronger and more direct role in the approval, oversight and review of the proposed governmental intervention power in cyber security incidents. This is particularly important given that the ED Bill proposes to confer legal immunities on officials who exercise powers of direction and intervention.

Oversight and review of administrative decisions and conduct

8. The Law Council is concerned that inadequate provision is made for independent oversight and review of the exercise of powers under the expanded regime. Statutory judicial review of the most significant powers would be excluded, and no merits review rights exist. Despite the significant proposed expansion of the regime, the existing secrecy provisions in the *Security of Critical Infrastructure Act 2018* (Cth) (**SCI Act**) will continue to apply, which purport to override the powers of courts, tribunals and oversight bodies to compel the disclosure of information, and prohibit disclosures to lawyers for the purpose of obtaining legal advice, and voluntary disclosures to Commonwealth integrity agencies. There is also no proposal to invest the Commonwealth Ombudsman with standing inspection functions in relation to the actions of the Department in exercising powers under the regime.

Preliminary issue: intended timing for legislative passage

9. The Law Council understands from the Department's advice at a public information session on the previous consultation paper in August 2020 that the Government, at that time, intended to introduce and seek passage of this legislation in 2020. However, only eight Parliamentary sitting days remain in 2020.

The need for adequate time for Parliamentary scrutiny

10. If there remains a desire to seek passage in 2020, the Law Council recommends that this position is revisited, to ensure that an adequate timeframe, in the nature of several months, is provided for Parliamentary scrutiny and debate.

11. This longer timeframe would be commensurate with the national significance of the proposed measures, together with their significant regulatory footprint and impacts on individual rights and liberties. It could avoid the need for multiple post-enactment reviews of, and the need for major remedial amendments to, legislation that is passed urgently with truncated scrutiny. This occurred with the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth), and the Law Council supports efforts to avoid any repetition of this outcome.

Importance of scrutinising proposed delegations of legislative power

12. Given the nature of the ED Bill as a high-level framework, which enables detailed regulatory obligations to be set in delegated legislation, a fundamental issue for the Parliamentary scrutiny of the Bill will be to determine the most appropriate division of matters to be dealt with in primary legislation and delegated legislation. The Parliament will also need to consider the conditions and other safeguards to be imposed on, or in relation to, the exercise of delegated legislative powers.

13. Consequently, the Law Council considers that a proposal to seek the near immediate passage of this legislation in 2020 could not credibly be justified on the basis that deferred commencement of the Act, up to six months after it receives royal assent, would provide an adequate, longer period for the Minister for Home Affairs (**Minister**) to develop statutory rules prescribing the substance of regulatory obligations, and for the Parliament to scrutinise and consider whether to disallow those legislative instruments.

14. While the Law Council supports the disallowable nature of the various sets of statutory rules required to be made under the new regime, disallowance is no substitute for the Parliament being given an adequate opportunity to scrutinise the nature, scope and terms of the legislative powers that it is being requested to delegate to the executive, and the immunities it is being asked to confer for acts done in good faith compliance or purported compliance.

15. In this regard, weight should also be placed on the fact that most of the subordinate legislative instruments will be rules rather than regulations, which will have a lesser degree of internal scrutiny in their development and approval, and will not be drafted by the Office of Parliamentary Counsel. The use of rules, rather than regulations, to prescribe important matters was of concern to the Senate Scrutiny of Delegated Legislation Committee in its 2019 report on its inquiry into the Parliamentary scrutiny of delegated legislation.[1] The Law Council considers that this proposal heightens

[1] Senate Standing Committee for the Scrutiny of Delegated Legislation, *Parliamentary Scrutiny of Delegated Legislation*, (March 2019), 92 at [5.39].

the need for detailed and thorough Parliamentary scrutiny of the proposed delegations of legislative power in a Bill.

16. Further, the ED Bill proposes that many of the essential requirements of the regime will be set by individual notices, directions and determinations issued by the Minister or Secretary of the Department, which are non-legislative instruments that are not required to be made public. Most of these instruments will be subject to the extensive non-disclosure provisions in the SCI Act.

17. Since it is therefore likely that the Parliament and wider public will have limited or no visibility of the exercise of these delegated powers, it is important that there is thorough scrutiny of the provisions of primary legislation which proposed to confer those powers and regulate their exercise. This includes the careful examination of applicable oversight, review and accountability mechanisms.

18. It will be particularly important that the Government does not seek to call on a Bill for Parliamentary debate and passage until all legislative scrutiny committees, including the Parliamentary Joint Committee on Human Rights and the Senate Scrutiny of Bills Committee, have concluded their consideration of the Bill, and there has been a reasonable opportunity for Parliamentarians to consider those reports.

19. The Law Council's strong preference for allocating an adequate amount of time for Parliamentary scrutiny is consistent with the caution recently sounded by the Senate Standing Committee on Delegated Legislation in its review of the Parliamentary scrutiny of delegated legislation. That Committee observed that many concerns it had identified in its scrutiny of legislative instruments could have be avoided if the Government had proposed, or the Parliament had insisted upon, placing stronger parameters on delegated legislative powers when developing and scrutinising Bills.[2]

Importance of scrutinising the novel, ministerial authorisation framework for governmental intervention in cyber security incident responses

20. Proposed Part 3A of the SCI Act seeks to establish a novel arrangement for governmental intervention in cyber security incidents affecting privately held critical infrastructure assets. In effect, it adopts domestically a similar ministerial authorisation (**MA**) framework to that governing the offshore activities of certain intelligence agencies under the *Intelligence Services Act 2001* (Cth) (**ISA**).[3]

21. The effect of the proposed MA framework (**SCI-Act MA regime**) is that the Secretary of the Department of Home Affairs (**Secretary**) will be authorised to issue a wide range of directions to critical infrastructure owners and operators, and to the Australian Signals Directorate (**ASD**) to intervene in the response to an incident. (However, the Law Council notes that the taking of offensive action to combat a cyber security attack is expressly excluded.)

22. The novel and complex nature of this arrangement, particularly in relation to oversight and safeguards, requires further explanation and context beyond the limited information provided in the explanatory document to the ED Bill. More time is also needed to scrutinise this aspect of the proposed regime than has been

[2] Ibid, Chapter 5, especially recommendations 8-10.

[3] ISA, Part 2, Division 1 (especially sections 8 and 9) which prescribes MA requirements for certain activities of the Australian Secret Intelligence Service (**ASIS**), Australian Signals Directorate (**ASD**), and Australian Geospatial-Intelligence Organisation (**AGO**). Generally, an MA will be required for activities of all agencies that involve the production of intelligence on an Australian person overseas, and certain activities of ASIS which will have a direct effect on an Australian person overseas. Ministerial authorisation is required for these acts, irrespective of whether they would otherwise constitute an offence or a tort. However, for those acts which would otherwise be unlawful or tortious, section 14 of the ISA confers an immunity from legal liability upon members of agencies who undertake acts in the proper performance of their agency's functions.

possible in the consultation period for the ED Bill, and more time than is available in the remaining eight Parliamentary sitting days in 2020.

Access to draft administrative materials in scrutinising the Bill

Regulation Impact Statement

23. The explanatory document accompanying the ED Bill (**Explanatory Document**) indicates that, while work is being done to assess the regulatory impacts of the expanded regime, and a 'qualitative' Regulation Impact Statement (**RIS**) has been prepared, there is no apparent intention to release a formal RIS for the Bill itself.[4]

24. Rather, there appears to be an intention to prepare an individual RIS accompanying each set of sector-specific statutory rules which prescribe regulated assets, and details of obligations with respect to risk management and incident response plans, vulnerability assessments and reporting requirements. It appears that these statutory rules would be prepared, and the accompanying RIS and other explanatory materials released, after the Bill has been passed.[5]

25. The Law Council would prefer to see the preparation and release of at least a high-level RIS accompanying the Bill, as well as an individual RIS accompanying each set of sector-specific statutory rules if the Bill is passed. Such transparency would considerably aid the scrutiny of the proposed legislation.

26. The Law Council derived assistance from the inclusion of a RIS in the explanatory memoranda to the Telecommunications and Other Legislation Amendment Bill 2016, which enacted the telecommunications sector security regime (**TSSR**) in Part 14 of the *Telecommunications Act 1997* (Cth) (**Telco Act**), and the Security of Critical Infrastructure Bill 2017, which enacted the SCI Act.

27. The Law Council acknowledges that the regimes in the SCI Act and Telco Act are presently limited to defined sectors. Nonetheless, the practice of releasing a RIS with the originating Bills to those Acts highlighted the utility of stakeholders having access to as much information as possible about projected regulatory impacts and the way in which they are being considered, as part of the process of scrutinising the originating Bills, and not only when later examining subordinate legislation prescribing further details to make the regime operational.

Other supporting administrative materials

28. The Law Council also considers that it would be desirable for the Parliament, industry, civil society and wider public to have access to draft administrative materials to support the implementation of the expanded regulatory regime, while a Bill is under consideration by the Parliament. This would ideally include:

- draft rules to be made under the proposed legislation, or at least statements of approach that outline core elements and guiding principles to promote substantive equality and consistency of treatment across different sectors;
- draft operational materials about the approach to monitoring and enforcing compliance, including details about the intended application of the Australian Government Regulator Performance Framework to the Department in relation to its administration of the expanded regime under the SCI Act; and

[4] Explanatory Document, 8 at [42].
[5] Ibid.

- draft guidance materials about decision-making in relation to requesting, approving and executing the SCI-Act MA regime for responses to serious cyber security incidents.

29. The Law Council understands that some details about the implementation and operation of the proposed regime, such as technical specifications in relation to system information and software, may be sensitive and the dissemination of draft guidance materials may need to be undertaken via secure means, such as the Trusted Information Sharing Network (**TISN**) for communications between government and industry on security related matters.

30. However, the types of administrative materials listed above, which the Law Council considers should be prepared and made available while the Parliament is scrutinising the Bill, are not directed to the disclosure of technical or otherwise sensitive operational or commercial information. Rather, they seek clarity about the intended regulatory approach under the proposed expansions to the SCI regime.

31. The Law Council notes that the release of such guidance materials during the Parliamentary scrutiny of a Bill can provide considerable assurance about the intended manner of operation of the regime. This can be relevant to stakeholder views and the Parliament's decision-making about the nature and scope of the discretionary powers sought to be delegated to members of the executive, and the matters that should be dealt with in primary legislation alone.

32. This was the case with the establishment of the TSSR measures in 2016-17, in which draft administrative guidelines were released and considered as part of the Parliamentary scrutiny of the Bill. This enabled the identification of areas of uncertainty for industry and other stakeholders, and the identification of priority areas by the Parliament in respect of which specific guidance was requested.[6]

Interaction with proposed foreign investment reforms

33. The Foreign Investment Committee (**FI Committee**) of the Law Council's Business Law Section (**BLS**) also wishes to register its concern with the apparent absence of coordination of public consultation processes for the proposed amendments to the regulatory regimes for critical infrastructure and foreign investment.

34. In August 2020, the FI Committee provided submissions to the Department of the Treasury, which commented on proposed amendments to the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (**FATA**), in the exposure draft of the *Foreign Investment Reform (Protecting Australia's National Security) Bill 2020* and associated exposure draft regulations proposed to be made under the FATA, as amended.

35. However, when the proposed changes to the FATA were first released, the proposed changes to the SCI Act had not been released. Accordingly, the full impact of those proposed changes was not apparent, including their impact on the proposed mandatory notifications under the FATA. Likewise, the RIS in relation to the FATA changes was prepared before the proposed changes to the SCI Act were finalised, meaning that it does not take account of the broader package of changes and their impacts, and that many persons who responded with submissions to the FATA changes did not have the opportunity to consider these important developments.

[6] See: Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications and Other Legislation Amendment Bill 2016*, (June 2017), especially recs 1, 4 and 12.

36. Accordingly, the Law Council supports a longer timeframe for the consideration of both sets of proposed amendments, so that their combined effects (including regulatory impacts) can be assessed.

Interactions with statutory reviews of critical infrastructure laws

37. Moreover, the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) is required to commence a statutory review of the SCI Act by 11 April 2021.[7] That review has not yet commenced. The PJCIS is required to consider the operation, effectiveness and implications of the Act; as well as whether it would be appropriate to have a unified scheme for all critical infrastructure assets, including telecommunications assets.[8]

38. Separately, the PJCIS is also undertaking a statutory review of the related TSSR for telecommunications carriers and carriage service providers and intermediaries in Part 14 of Telco Act, which is required to report by 18 September 2021.[9]

39. The Law Council considers that the major reforms proposed to the SCI Act in the ED Bill would ideally be considered as part of, or in coordination with, these statutory reviews of the existing regulatory regimes.

40. This would enable evidence of current experience to inform the development of the proposed expansions, and for the proposed expansions to be assessed holistically, as a component of a broader national regulatory framework. This will also help to avoid risks of fragmentation or inconsistent treatment between entities regulated by the SCI Act and the TSSR measures in the Telco Act respectively.

Recommendation 1—adequate opportunity for Parliamentary and public scrutiny

- **If a Bill is introduced to Parliament in 2020, passage should not be sought until the Autumn 2021 sittings, to enable thorough scrutiny (including the combined impact of the proposed amendments to security of critical infrastructure and foreign investment laws).**
- **This should include adequate time for all legislative scrutiny committees, including the Parliamentary Joint Committee on Human Rights and the Senate Scrutiny of Bills Committee, to report and for members to consider those reports.**

Schedule 1: amendments to the Security of Critical Infrastructure Act 2018 (Cth)

Key proposed amendments

41. The Law Council notes the following proposed expansions of the regulatory regime.

- **The imposition of an expanded 'positive security obligation' on the owners and operators of critical infrastructure assets, which:**
  - expands the range of critical infrastructure sectors and assets able to be regulated under the regime (namely, a total of eleven sectors, with individual assets that 'relate to' those sectors being covered). Certain regulatory obligations may be 'turned on' for particular assets via the

[7] SCI Act, section 60A.
[8] Ibid, subsection 60A(1).
[9] Telco Act, section 315K.

making of statutory rules by the Minister, or by private Ministerial declaration if certain security-related grounds exist;

- imposes further obligations on regulated entities, which are enforceable by civil penalty provisions. The new regulatory obligations are additional to the existing obligations in the SCI Act with respect to reporting and notification, and complying with Ministerial directions to take, or refrain from taking, specified action on security grounds. They cover:

  - requirements to develop, comply with, report on and periodically review and update 'critical infrastructure risk management programs', which identify material hazards and mitigation or elimination strategies (and comply with any other matters set out in rules made by the Minister); and

  - requirements to provide notification if a cyber security incident occurs which has a 'relevant impact' on the operation of a critical infrastructure asset (essentially a direct or indirect impact, of any magnitude, on the availability, integrity and reliability of the asset, or a direct or indirect impact on the confidentiality of information about the asset or information stored in the asset or in a computer);

- **The imposition of specific cyber security obligations in relation to 'systems of national significance'**

  The new concept of a 'system of national significance' will cover a critical infrastructure asset that is declared, in writing, by the Minister in a non-legislative instrument, if the Minister is satisfied the asset is a 'system of national significance' (having regard to interdependencies between the asset and other critical infrastructure assets, and any other matters they consider relevant). The additional obligations are:

  - ***incident response planning obligations***, including requirements to develop, comply with and review and update an incident response plan for cyber security incidents; to conduct and report on cyber security exercises as directed by the Secretary;

  - ***requirements to conduct and report on vulnerability assessments*** in relation to computer systems and cybersecurity generally, as directed by the Secretary; and

  - ***requirements to report periodically on system information***, which relates to the operation of a computer that is used to operate a system of national significance, including requirements to install system information software, as directed by the Secretary;

- **The conferral of additional enforcement powers on the Secretary of the Department in relation to all of the new and existing obligations**

  The ED Bill proposes to enliven additional enforcement powers in the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) (**RPA**) to confer monitoring, investigation and infringement notice powers on the Department of Home Affairs. This is additional to the enforcement powers in existing section 49, which enliven the civil penalty, enforceable undertaking and injunction provisions of the RPA.

- **The establishment of an MA regime for government intervention in serious cyber attacks on privately held critical infrastructure assets**

While these powers are labelled 'assistance' they are more accurately characterised as intervention, because they are exercisable in the absence of the agreement or request of the owners or operators of privately held critical infrastructure assets. The proposed regime operates on the following basis:

- the Minister issues an SCI-Act MA, on the oral or written application of the Secretary, if satisfied that:
  - a cyber security incident has occurred, is occurring or is imminent;
  - that incident is likely to have a relevant impact on a critical infrastructure asset;
  - there is a material risk of serious prejudice to Australia's social or economic stability, defence or national security;
  - no existing Commonwealth, State or Territory regulatory system could respond adequately; and
  - the Minister is satisfied that various directions able to be given under the MA are likely to facilitate a practical and effective response to the incident;
- the SCI-Act MA may authorise the Secretary to do one or more of the following, for up to 20 days:
  - issue directions to an owner or operator of a critical infrastructure asset to take action or omit to take action, or to provide information; and
  - request ASD to intervene, if satisfied that this is reasonably necessary and proportionate, technically feasible, and the infrastructure owners or operators are unwilling or unable to take action themselves.

  ASD's acts of intervention may include the following (in respect of which it is conferred with immunity from criminal or civil liability for acts done in good faith compliance, or purported compliance, with the SCI-Act MA):
  - accessing or modifying data held in a computer that is part of the critical infrastructure asset to which the SCI Act-MA relates;
  - undertaking an analysis of a computer, or computer program or data; and
  - doing incidental acts including accessing, adding, copying, altering or deleting data; altering the function of a computer; removing or disconnecting a computer; connecting another computer, temporarily removing a computer from premises, and entering premises (including with the assistance of a constable, who is authorised to use force against property for this purpose).

Summary of Law Council position on Schedule 1 measures

42. The Law Council does not oppose, in principle, the establishment of a coordinated and nationally consistent regulatory regime for the protection and resilience of critical infrastructure assets within Australia, from all forms of security risks. However, the regulatory burden and associated limitations on rights and liberties must go no further than is necessary, reasonable and proportionate.

43. The Law Council notes that the proposed expansion of the SCI regime appears to be unprecedented among Australia's Five Eyes counterparts. Moreover, it is important to acknowledge that the proposed expanded regime would not operate in a comparable constitutional and legislative framework for the protection of human rights as those which exist in all other Five Eyes jurisdictions.

Key issues

44. The Law Council comments on matters of detail in the proposed regime, which focus on the following core areas:

Delegations of legislative power

- broad delegations of legislative power with limited statutory parameters for its discretionary exercise, particularly in relation to prescribing the assets covered by the regime, details of security obligations in relation to those assets, and the determination of a cyber security incident to be 'serious' for the purpose of enlivening the SCI-Act MA regime;

Thresholds and scope of powers, including enforcement

- imprecise or low thresholds for the exercise of coercive and intrusive powers, including enforcement (particularly the conferral of investigative and monitoring powers on the Department of Home Affairs, with wide powers of delegation in relation to enforcement functions);

Review rights

- limitations on legal rights of review of administrative decisions made under the proposed expanded regime, namely:
  - limitations in judicial review rights, primarily:
    - the exclusion of statutory judicial review rights in relation to all decisions made under the proposed SCI-Act MA regime in new Part 3A of the SCI Act, based on a generalised appeal to national security considerations; and
    - the impact of highly restrictive secrecy provisions in section 47 of the SCI Act that will likely prevent the effective exercise judicial review rights in original jurisdiction; and
  - the absence of any merits review rights (for example, rights to seek review in the Security Division of the Administrative Appeals Tribunal);

Immunities from civil and criminal liability

- the scope of proposed immunities from civil and criminal liability for persons performing functions or exercising powers under the expanded regime;
- a potentially unintended result in relation to ASD, which will mean that it is conferred with multiple immunities under multiple statutes, however:
  - each immunity will differ in its scope. In particular,
    - the proposed immunity in the SCI Act will not be contingent on the 'proper performance' by ASD of its functions, which is one of the requirements for the existing immunities conferred under section 14 of the *Intelligence Services Act 2001* (Cth) (**ISA**) and Part 10.7 of the *Criminal Code Act 1995* (Cth) (**Criminal Code**); and

        - the immunities in the ISA and Criminal Code are also subject to evidentiary certification powers by the Inspector-General of Intelligence and Security (**IGIS**) in respect of whether ASD engaged in an activity in the proper performance of its functions. A much broader certification function applies in relation to the proposed SCI Act immunity, covering any fact. The Law Council is concerned about the appropriateness of the proposed establishment of such a broad certification arrangement, and the proposed conferral of that certification function on the IGIS; and

    - the proposed immunity in the SCI Act will not require ASD to notify the IGIS when ASD relies on that immunity and knows that a third party has suffered, or is likely to suffer or to have suffered, material loss or damage as a result of ASD's actions. This is in contrast to the proposed notification obligations in Schedule 2 to the ED Bill, in relation to ASD's immunity under Part 10.7 of the Criminal Code;

Operational oversight

- limitations on independent operational oversight of the expanded regime, particularly the functions of the Commonwealth Ombudsman in overseeing the actions of the Department of Home Affairs in administering the regime. This includes the following key issues:
    - the absence of a statutory basis for the Commonwealth Ombudsman to conduct inspections of the Department of Home Affairs in relation to its administration of the regime;
    - the application of the secrecy provisions in existing sections 45-47 of the SCI Act to an expanded range of information:
        - section 46 does not presently contain any exceptions to the secrecy offence in section 45 for voluntary disclosures to Commonwealth oversight bodies with relevant responsibilities; and
        - section 47 purports to override the coercive information-gathering powers of those bodies.

      The ED Bill does not propose any consequential amendments to these provisions to accommodate a genuine need for enhanced oversight as a result of the broader powers, obligations and liabilities proposed to be conferred; and
    - the absence of consequential amendments to the secrecy provisions in section 34 of the *Inspector-General of Intelligence and Security Act 1986* (Cth) (**IGIS Act**) to remove conflict between the prohibitions on disclosure of information in that provision, and the permitted disclosures to the Commonwealth Ombudsman under proposed section 43B of the SCI Act (per item 50 of Schedule 1 to the ED Bill); and

Statutory reviews of the expanded regime

- the absence of statutory provisions requiring independent or Parliamentary reviews (or both) in relation to the operation of the expanded regime, after it has been in force for a reasonable period, such as three years.

  For example, the ED Bill does not propose to update or expand upon the present, one-off statutory review provision in existing section 60A of the SCI Act, which requires the PJCIS to commence a review of that Act in 2021.

Caveat

45. In view of the limited timeframes for consultation on the ED legislation, and the significant volume of legislation presently the subject of Parliamentary inquiry or public consultation, these issues are not necessarily exhaustive or conclusive of the Law Council's position.

Expanded positive security obligations, and cyber security obligations for 'systems of national significance'

Scope, thresholds and contents of obligations

46. The expanded security obligations in proposed Parts 2A and 2B, together with the expanded definition of 'critical infrastructure asset' (and component terms) confer significant delegations of legislative power to prescribe the entities which are covered, and the substance of their regulatory obligations under Parts 2, 2A, 2B, 3 and 3A of the SCI Act (as proposed to be amended).

47. While the Law Council recognises the interests in flexibility, including to take account of changes in the nature of assets and sectors and their attendant capabilities and security risks, it considers that further statutory parameters are needed, including:

- consideration of whether further matters can be placed in primary legislation as criteria for the exercise of delegated legislative powers. This should include consideration of the following matters:
  - a statutory pre-condition for protocols to have been made detailing the process for rule-making under the SCI Act; and
  - a statutory pre-condition to identify and take into consideration the impacts of proposed new or amended rules on broader regulatory regimes, including with respect to foreign investment (**see below**);
- more extensive consultation requirements in relation to proposed rules, which relevantly provide for:
  - longer consultation periods than the proposed period of 14 days, which the Law Council considers is disproportionate to the significant regulatory impacts of the proposed rules on regulated entities as well as third parties), and the highly technical nature of the SCI regime;
  - more extensive requirements to notify relevant entities of proposed regulatory changes than the proposed requirement to cause a notice to be placed on part of the Department's website (which may be unlikely to come to the attention of entities affected by the proposed rules, and may compound the inadequate statutory minimum consultation period);
  - express statutory obligations on the Minister to take into account consultation comments before making rules;
  - an express provision stating that rules are invalid if the Minister has failed to comply with all of the statutory consultation requirements; and
  - stronger limitations on the Minister's power to bypass consultation requirements in circumstances of emergency. This should include requirements directed to ensuring the necessity and proportionality of such a course of action, such as the following matters:

- requirements for the Minister to be satisfied that an incident which has occurred (or is imminent) will not only have a significant impact on an asset; but will also be likely to cause serious prejudice to national interests, or otherwise have significant, adverse effects on third parties that rely on the asset; and

- requirements for the Minister to consider the potential impacts on regulated entities of failure to consult; and to weigh these against the assessment of the gravity and likelihood of harm to essential national interests that may arise from delay in issuing rules as a result of a consultation process; and

- stronger safeguards in relation to the operation of the rules in respect of which the Minister has bypassed the general consultation requirements. For example:

  - such rules should sunset within a fixed, short-term period (in the nature of months) so that they are not in force any longer than is necessary for the immediate response to a particular incident;

  - the Minister should be under an explicit statutory obligation to conduct consultations on permanent / ongoing rules, and to revoke the temporary / emergency rules at the first available opportunity;

  - some form of legal protection against enforcement action (such as an exception or defence of reasonable excuse) should apply in relation to regulated entities that fail to comply with their obligations under rules that were not the subject of consultation, if compliance with those obligations would have been impossible, or would have exposed the entity to significant hardship;

- consideration should be given to statutory mechanisms to improve Parliamentary scrutiny and control over the exercise of the proposed rule-making powers, in recognition of their expansive scope and the gravity of their impacts on regulated entities and others. This should include consideration of the following amendments to the Bill:

  - the insertion of provisions which defer the commencement of statutory rules (except in emergencies) until after the expiry of the Parliamentary disallowance period, rather than commencement immediately upon registration on the Federal Register of Legislation.

    Deferred commencement would maximise the opportunity for meaningful Parliamentary scrutiny of the rules. Importantly, it would mean that the Parliament would not have to weigh any concerns it may have with the substance of rules with the regulatory impact on industry of repealing rules that are already in force. (Noting that regulated entities are likely to have incurred significant expense in their structuring their compliance arrangements around the rules.) Rather, Parliament would be free to examine the rules purely on the merits of their substance, without having to additionally take into account the impacts of disallowance if the rules were already binding on regulated entities; and

  - provisions which confer functions on the PJCIS (or another Parliamentary Committee) to conduct inquiries into statutory rules made under the SCI Act, and to make advisory recommendations about the exercise (or otherwise) of disallowance powers. One reason it may be

advantageous to confer such a function on the PJCIS is the ability of that Committee to receive classified evidence;

48. As discussed subsequently in relation to secrecy provisions, in the context of review and oversight, consideration should also be given to whether there is a need for further permitted disclosures in section 46 of the SCI Act, to facilitate effective consultation in relation to proposed rules. For example, regulated entities that are affected by proposed rules may need to disclose 'protected information' for the purpose of obtaining legal advice on those proposed changes. They may also need to consult with third parties that use their assets, or which provide services to them, to ascertain the impacts of proposed rules.

Recommendation 2—stronger parameters on proposed delegations of power in respect of expanded security obligations

- **The ED Bill should be revised to take account of the matters set out at paragraphs [47] and [48] of this submission in relation to the proposed delegation of legislative powers to the Minister.**

Interaction with proposed amendments to foreign investment laws

49. The FI Committee of the Law Council's BLS made submissions on 31 August 2020 to the Department of the Treasury on exposure drafts of:

- proposed amendments to the FATA in the Foreign Investment Reform (Protecting Australia's National Security) Bill 2020; and
- the Foreign Investment Reform (Protecting Australia's National Security) (National Security Business) Regulations 2020 (**National Security FATR**).

50. In those submissions, the FI Committee recommended that the proposed cross-referencing to critical infrastructure assets under the SCI Act in section 10A of the draft National Security FATR be fixed to the **current list** of critical infrastructure assets, without automatic updating or the current definition of critical infrastructure assets be replicated in the draft National Security FATR as a standalone category.

51. The FI Committee is now even more concerned about the proposed cross-referencing, having reviewed the ED Bill. The proposed expansion of the concept of 'critical infrastructure assets' in the SCI Act to cover an additional 11 sectors will capture an extraordinarily broad range and number of businesses. It will not always be the case that the acquisition of a 'direct interest' (generally a 10 per cent or greater interest) in any such business raises any actual or potential national security issues so as to justify a mandatory notification requirement under the Foreign Investment Review Board (**FIRB**) regime.

52. The FI Committee notes that, by seeking to define 'critical infrastructure assets' for the purposes of the FATA by reference to the SCI Act, the Government avoids the difficult task of:

- considering which of the additional sectors, and businesses within those sectors, proposed as critical infrastructure assets for the purposes of the SCI Act should be considered as national security businesses for the purposes of the FATA; and

- identifying whether there are ambiguities in the proposed amendments to the SCI Act in the ED Bill, which need to be clarified, both for the purposes of the SCI Act and the FATA. By way of non-exhaustive examples of ambiguities:

- the proposed definition of 'critical data storage or processing asset' seems to apply to the owner of property on which a data centre is based and to equipment providers who provide IT for the data centre. However, the FI Committee understands that the intent is that it applies only to those actually involved with the operation of the data centre; and

- the ED Bill proposes to amend the SCI Act to confer delegated legislative powers to effectively 'turn on' and 'turn off' the regulatory regime under that Act in relation to a particular asset (by prescribing or 'de-prescribing' it as a 'critical infrastructure asset'). However, it is not clear whether the FATA (as is proposed to be amended) will capture the effect of rules made under the SCI Act (as proposed to be amended) which effectively change the definition of 'critical infrastructure asset' under the SCI Act.

53. Although this task may be difficult, the FI Committee considers that it is necessary for the effective operation of both the foreign investment and SCI regimes. It should be done in consultation with the business community and other stakeholders, to ensure that there remains an appropriate balance between protecting against national security risks and not deterring foreign investment.

54. Otherwise there will undoubtedly be an exponential increase in the number of applications submitted to FIRB, well beyond the figures put forward in the regulation impact section of the explanatory memorandum to the Foreign Investment Reform (Protecting Australia's National Security) Bill 2020 which stated that 'It is estimated that the reforms will result in around 100 additional applications and 1,800 additional registrations being made by investors each year, involving an additional aggregate compliance cost of approximately $1.5 million per annum, on average'.

55. The FI Committee believes that the figure will be more in the ballpark of at least 1,000 additional applications each year. Unless FIRB is given substantial additional resources, this will unavoidably mean lengthy FIRB processing times and possible loss of foreign investment to other jurisdictions, which is not in anyone's interests.

56. Accordingly, it will be crucial that the Government provides the business community with a reasonable opportunity to provide submissions on the proposed definition of 'critical infrastructure assets' for the purposes of both the SCI Act and the FATA, and to reconsiders its cross-referencing proposal having regard to such submissions.

57. The Law Council recommends that these matters are taken up in addition to the recommendations above, which are directed to setting stronger statutory parameters on the proposed delegations of legislation power under the SCI Act to determine the application of the regime to specific assets, and the content of applicable obligations.

Ministerial authorisation regime for governmental intervention in serious cyber security incidents ('SCI-Act MA regime')

Thresholds and process for issuing an SCI-Act MA

58. The SCI-Act MA regime in proposed Part 3A of the SCI Act is similar, in many respects, to the MA regime in the ISA in relation to the overseas intelligence collection activities of ASD, the Australian Secret Intelligence Service (**ASIS**), and the Australian Geospatial-Intelligence Organisation (**AGO**) in relation to activities that involve the production of intelligence on Australian persons in foreign countries (**ISA-MA regime).**

59. However, the key differences between the ISA-Act MA regime, and the proposed SCI-Act MA regime, are that the proposed SCI-Act MA regime:

- will authorise acts inside Australia;
- will authorise those acts inside Australia for the purpose of responding to a 'serious cyber security incident' affecting privately held critical infrastructure assets in Australia, rather than the overseas collection of intelligence about Australian persons, which is relevant to Australia's interests;
- will be administered by the Home Affairs portfolio, with the Home Affairs Minister issuing MAs on the application of the Secretary of the Department;
- will confer wide discretionary powers on the Secretary about the acts to be undertaken pursuant to the SCI-Act MA, including the exercise of coercive powers against owners and operators of critical infrastructure assets;
- will require ASD to perform (non-offensive) intervention functions at the behest of another portfolio Minister (and Secretary of that portfolio Department) rather than its own Minister, on its direct request for authorisation; and
- will authorise SCI-Act MAs to remain in force for up to 20 days, which in the absence of explanation is difficult to reconcile with the stated policy intention that the extraordinary intervention powers proposed to be conferred under SCI-Act MAs are directed to circumstances of urgency and emergency.

Recommended improvements

60. There are a number of positive aspects of the proposed powers to issue and make directions under SCI Act MAs, including:

- a limitation of the power to incidents which are likely to cause **serious** prejudice to specified national interests;
- explicit requirements to be satisfied of the necessity and proportionality of the powers sought to be authorised, including statutory guidance in applying the test of proportionality;
- a requirement for the Minister to consult with the responsible entity or entities for the relevant critical infrastructure asset or assets, before issuing an SCI-Act MA; and
- while there is no limitation on the number of subsequent SCI-Act MAs that can be issued in relation to an incident, the Minister is required to take into account the number of occasions on which an MA was issued previously.

61. However, the Law Council is concerned about overbreadth in several aspects of the issuing threshold and process for SCI-Act MAs and recommends various amendments, as set out below.

Independent issuing

62. Consideration should be given to an independent issuing process, noting the recommendations of the third Independent National Security Legislation Monitor (I**NSLM**), Dr James Renwick SC, in relation to the compulsory industry assistance regime in Part 15 of the Telco Act (as enacted by the TOLA Act in 2018).

63. The third INSLM recommended independent issuing (by a new Investigatory Powers Division of the Administrative Appeals Tribunal, headed by a retired judge) of the extraordinary powers of coercion able to be exercised against private industry, having regard to the gravity of those powers and the need for the highest levels of public and industry trust and confidence in the integrity of that regime.

64. The Law Council considers that the considerations identified by the third INSLM apply equally to the proposed intervention regime in new Part 3A of the SCI Act. The proposed SCI intervention regime is fundamentally distinguishable to the matters to which the MA model in the ISA is directed. Namely, the proposed SCI-related intervention powers will:

- apply domestically, and will therefore affect Australian persons who are physically present in Australia. This includes the application of immunities for acts done under, or in purported compliance with, an SCI-Act MA (which will extinguish the rights of Australian persons to legal remedies in relation to any loss, damage, injury or harm suffered as a result of interventions); and
- confer powers of coercion that require private entities to engage or refrain from engaging in particular actions and provide certain information, not merely intrusive surveillance powers.

65. The Law Council submits that these factors mean that the model proposed by the third INSLM in relation to the compulsory industry assistance regime in the Telco Act is a preferable basis for the new SCI intervention regime than the MA regime in the ISA for intelligence collection purposes.

Recommendation 3—issuing authority for intervention powers

- **Consideration should be given to an independent issuing authority for authorisations to exercise powers of direction and intervention under new Part 3A of the SCI Act, along the lines recommended by the third INSLM in relation to the authorisation of compulsory industry assistance powers under Part 15 of the Telco Act.**

Issuing threshold

66. While the Law Council supports the proposed threshold of 'serious prejudice' to specified national interests, it is concerned that the national interests which are specified in proposed paragraph 35AB(1)(c) are extremely broad and vague, and appear to duplicate and overlap with each other in several respects.

Australia's social and economic stability

67. For example, the concept of 'social or economic stability' in proposed subparagraph 35AB(1)(c)(i) is undefined, and its ordinary meaning could cover a wide and uncertain (and potentially indeterminate) range of matters. The rule of law requires that the law must be readily known and available and certain and clear. This requires that key terms be defined with precision, especially in relation to thresholds for the exercise of coercive and intrusive powers.

The defence of Australia

68. The concept of 'defence of Australia' is recognised explicitly in proposed subparagraph 35AB(1)(c)(ii). However, proposed subparagraph 35AB(1)(c)(iii) covers the concept of 'national security' which is defined in existing section 5 of the SCI Act as 'Australia's defence, security and international relations'.

69. In addition to the duplication of the concept of 'defence' in proposed subparagraphs (ii) and (iii) of paragraph 35AB(1)(c), it is unclear why the proposed intervention powers need to be available for the purpose of the conduct of Australia's relations with foreign governments. The Explanatory Document does not address the necessity or proportionality of this aspect of the proposed SCI-Act MA regime.

Meaning of 'national security': importation of the definition of 'security' in the ASIO Act

70. Further, existing section 5 of the SCI Act defines 'security' (as a component of the term 'national security' as used in new section 35AB) by reference to the definition of that term in section 4 of the ASIO Act, which is extremely broad, covering, among other matters:

(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.

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

- 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 SCI regime, including in relation to the SCI-Act MA regime in new Part 3A; and

- no justification has been offered for the proposal to extend the SCI-Act MA regime to the **matters in paragraph (b) of the definition of security in the ASIO Act** (that is, the fulfilment of Australia's obligations to other countries). The Law Council considers that the conferral of coercive powers for this purpose is neither necessary nor proportionate to a legitimate objective.

Meaning of 'offensive cyber action'

72. The Law Council welcomes the proposed exclusion in new subsection 35AB(12) of 'offensive cyber action' from the activities that ASD or a private owner or operator of critical infrastructure may be required to perform under an SCI-Act MA.

73. However, the ED Bill does not define the expression 'offensive cyber action'. The Law Council is concerned that, in practice, the distinction between a 'defensive' and an 'offensive' action may not always be clear, and interpretations may reasonably differ. The Law Council recommends that an attempt is made at a statutory definition of this term (even if this is done on a non-exhaustive basis) to facilitate clarity to the maximum extent possible.

Recommendation 4—definitional matters relevant to issuing thresholds

- **The definitions of key terms in the issuing criteria for SCI-Act MAs in proposed section 35AB of the SCI Act should be amended to address the matters of ambiguity, overbreadth and overlap identified above.**

  As a minimum:

  - **the definition of 'security' as a component term of 'national security' for the purpose of proposed subparagraph**

35AB(1)(c)(iii) should exclude paragraph (b) of the definition of security in the ASIO Act;

- **the reference to 'defence' in proposed subparagraph 35AB(1)(c)(ii) should be omitted, given that it is covered by the defined term 'national security' in proposed subparagraph35AB(1)(c)(iii);**
- **consideration should be given to the necessity and proportionality of allowing SCI-Act MAs to be issued in relation to matters causing serious prejudice to Australia's foreign relations, noting that this concept is covered by the definition of 'national security' in section 5 of the SCI Act, as used in proposed subparagraph 35AB(1)(c)(iii);**
- **express statutory limitations should be applied to the requesting and issuing of SCI-Act MAs on the basis of national security that is constituted by 'politically motivated violence' (as a component of the definition of 'security' in the ASIO Act, which is incorporated by reference in the definition of 'national security' in section 5 of the SCI Act). These limitations should place additional limitations on the power to issue SCI-Act MAs in relation to legitimate acts of protest, advocacy and dissent (especially cases in which lawful protestors are not themselves engaging in harmful or violent acts, but their actions may incite counter-protestors who engage in such acts);**
- **the term 'offensive cyber activity' for the purpose of the exclusion in proposed subsection 35AB(12) should be defined, so as to provide clarity and certainty; and**
- **the terms 'social stability' and 'economic stability' for the purpose of proposed subparagraph 35AB(1)(c)(i) should be defined, so as to provide clarity and certainty.**

Application of necessity and proportionality tests for authorised acts

74. The Law Council welcomes the inclusion of proposed subsections 35AB(5)-(7), which require the Minister to be satisfied of the necessity and proportionality of the proposed actions authorised under an SCI-Act MA requested by the Secretary.

75. However, this is not a complete assessment of the requirements of necessity and proportionality. The Law Council recommends that the Ministers should also be required to undertake a **cumulative assessment** of the necessity and proportionality of **all** of the individual powers proposed to be conferred under the MA. The Minister should not be authorised to issue an SCI-Act MA unless satisfied of the necessity and proportionality of the cumulative powers proposed to be conferred, as well as the individual necessity and proportionality of each power.

Recommendation 5—application of issuing tests of necessity and proportionality

- **Proposed subsections 35AB(5)-)(7) of the SCI Act should be amended to require the Minister to undertake an assessment of the cumulative necessity and proportionality of all of the powers proposed to be authorised under an SCI-Act MA, in addition to individually assessing the necessity and proportionality of each proposed power.**

Evidentiary basis and consultation requirements

76. There are no evidentiary thresholds for the Minister's satisfaction of the relevant conditions in proposed section 35AB.

77. Further, while there are some consultation requirements in relation to proposed MAs (namely, with the Prime Minister, Defence Minister and owners or operators of relevant critical infrastructure assets), the Law Council considers that these requirements do not go far enough to ensure that decisions are made on the basis of sufficient evidence and take into account all relevant considerations.

78. To address these matters, the Law Council recommends that the statutory conditions are strengthened in line with the recommended measures below. They would be additional to the proposed requirements in the ED Bill for the Minister to be satisfied of the matters specified in existing subsections 35AB(1)-(10). Namely:

- the Minister should be required to obtain the agreement of the Prime Minister and Defence Minister to the proposed SCI-Act MA, not merely to consult with them (as this means that the Minister would retain a statutory power to act contrary to their advice, or fail to consider it in making an issuing decision);
- the Minister should also be required to obtain the agreement of the Attorney-General to a proposed SCI-Act MA, given the Attorney-General's responsibility for human rights and integrity policy (as well as their experience in approving ASIO's warrant requests, which seek to engage in intrusive activities on the basis of security);
- consideration should be given to a certification requirement, as a pre-condition to requesting and issuing an SCI-Act MA, which requires certification from:
  - the Director-General of ASD as to:
    - the existence of a 'serious cyber security incident';
    - the need for the proposed intervention;
    - the technical feasibility and potential impacts of any proposed directions to be issued to critical infrastructure owners or operators; and
    - the fact that any proposed powers to require ASD's intervention will not involve the taking of 'offensive cyber action'; and
  - the Director-General of Security in relation to the likelihood that the cyber incident will cause serious prejudice to national security;
- all MA requests must be accompanied by a statement of facts and grounds (as is required for ASIO's warrant requests under section 28 of the ASIO Act); and
- there must be, in force, a protocol issued by the Minister for the making and determination of requests for SCI-Act MAs, with the following attributes:
  - ideally, the protocol would be available publicly, preferably as a legislative instrument, or at least published administratively (as is the case for the protocol for the listing of terrorist organisations under Division 102 of the Criminal Code); and
  - if publication of a protocol (in full or in part) is not compatible with requirements of security, then a copy of any classified protocol (or classified portions of a protocol) should be given to the IGIS, Commonwealth Ombudsman, Opposition Leader and PJCIS. Unclassified parts should be shared publicly.

Recommendation 6—evidentiary and consultation requirements

- **Section 35AB of the SCI Act should be amended to address the matters listed at paragraph [78] of this submission.**

Documentation requirements for SCI-Act MAs that are issued orally

79. The Law Council understands the need for an oral issuing power in circumstances of extreme emergency. It welcomes the approach to framing the power to make oral SCI-Act MAs in proposed section 35AE, which applies a general prohibition on oral issuing, subject to an exception if the Minister is satisfied that the time taken to give the authorisation in writing would frustrate the actions sought to be taken.

80. The Law Council also welcomes the requirements in proposed section 35AE for the Minister to make a written record of an oral SCI-Act MA, and ensure that copies are given to the relevant critical infrastructure owner or operator as well as the IGIS (in relation to oversight of ASD).

81. However, the Law Council is concerned about the following matters:

- ***the time limit for making a written record (48 hours after the oral issuing decision) is too long,*** given that the Secretary may conceivably issue directions immediately in view of the circumstances of urgency in which an oral SCI-Act MA is intended to operate. The Law Council recommends a much shorter time limit, in the nature of **one or two hours,** so that action taken under an SCI-Act MA does not commence in the absence of a written record of that MA. This would be commensurate with the conceivable complexity in the conditions of an SCI-Act MA, and the gravity of the powers of coercion and intervention conferred. These factors make it critical that there is a written record of the scope of powers conferred under an SCI-Act MA before those powers are exercised;

- ***there is no requirement for the Commonwealth Ombudsman to be given a copy of the SCI-Act MA, or be alerted to the Secretary's request for the MA.*** This is anomalous, since it is the Ombudsman, and not the IGIS, which has oversight responsibility for the actions of the Secretary in requesting an SCI-Act MA and issuing directions under that MA.

  While there may be a subjective policy intent that the IGIS will use their power under proposed section 43B of the SCI Act to disclose SCI-Act MAs to the Commonwealth Ombudsman, reliance on the discretion of the IGIS from time-to-time is not compatible with the separate and independent oversight functions of the Ombudsman in relation to the Department.

- ***there is no requirement for the Director-General of ASD to be given a copy of the SCI-Act MA***. Rather proposed section 35AX only requires the Secretary to include a statement in a request for ASD to undertake an intervention activity that the actions requested are in compliance with an underlying SCI-Act MA. The Law Council considers that ASD should be legally guaranteed access to the MA instrument itself, so that it can form an assessment as to whether the powers it is asked to exercise are lawful and proper, having direct regard to the scope of the source of authority.

Recommendation 7—requirements for oral authorisations

- **Proposed section 35AE (and related provisions) of the SCI Act should be amended to address the matters identified at paragraph [81] of this submission.**

Duration of SCI-Act MAs

82. The Law Council considers that further explanation is required for the proposed 20-day maximum duration of SCI-Act MAs in proposed section 35AG, having regard to the fact that the regime is intended to operate in emergencies.

83. The Law Council seeks reasons for the selection of 20 days and not a shorter period, including by reference to an evidence base that draws upon the duration of previous serious cyber security incidents that affected critical infrastructure assets.

Recommendation 8—further information about proposed maximum duration

- **The Government should provide further explanation of the proposed 20-day maximum duration for SCI-Act MAs, which draws upon evidence of the duration of previous serious cyber security incidents that affected critical infrastructure assets, and were assessed as causing or being likely to cause prejudice to the national interests specified in proposed paragraph 35AB(1)(c) of the SCI Act.**

Secretary's powers of direction under an SCI-Act MA

84. The Law Council welcomes the inclusion of several requirements new Part 3A in relation to the exercise by the Secretary of powers of direction under an SCI-Act MA. These include:

- requirements in proposed Divisions 3-5 of new Part 3A of the SCI Act, under which the Secretary must consider and be satisfied of the necessity and proportionality of proposed directions;
- requirements to consult with the owners or operators of critical infrastructure assets prior to issuing directions; and
- the proposal in item 68 of Schedule 1 to the ED Bill to exclude the Secretary's functions and powers under new Division 3A from the general powers of delegation.

85. However, the Law Council recommends several additional safeguards, as set out under the subheadings below.

Assessment of the necessity and proportionality of proposed directions

86. As with the above recommendations about the issuing thresholds for SCI-Act MAs, the Law Council also considers that the Secretary should be required to asses the combined impacts of all directions issued in relation to the responsible entity for an asset, in addition to the individual assessment of each intended direction.

87. This will ensure that the tests of necessity and proportionality are applied in an accurate and holistic manner.

Recommendation 9—application of necessity and proportionality tests

- **Divisions 3-5 of new Part 3A of the SCI Act should be amended to require the Secretary to consider the necessity and proportionality of the combined effect on regulated entities and third parties of each proposed direction or intervention request they intend to give under an SCI-Act MA, in addition to the necessity and proportionality of each individual direction or request.**

Oversight by the Commonwealth Ombudsman

88. As discussed separately below in relation to oversight, it is problematic that there is no proposal in the ED Bill to invest the Commonwealth Ombudsman with an inspection function (and associated powers of access to relevant information) in relation to the Secretary's actions in respect of SCI-Act MAs.

89. While the IGIS has a standing inspection function under the IGIS Act, it does not extend to the actions of the Secretary in requesting or exercising authority under an SCI-Act MA, as the functions of the IGIS are limited to six intelligence agencies.

90. While the Ombudsman has functions under the *Ombudsman Act 1976* (Cth) (**Ombudsman Act**) to investigate matters relevant to the actions of the Secretary (and persons assisting them) under new Part 3A, including in response to complaints, there is no pro-active function to access Home Affairs' systems to conduct ongoing scrutiny of the case underlying an SCI-Act MA request, and to assess the actions of the Secretary in issuing directions or requesting ASD's intervention.

91. In contrast, the IGIS performs these inspection functions in relation to MAs issued under the ISA, and will also have oversight of ASD's actions under intervention requests issued by the Secretary, but not the requests themselves (since Home Affairs is not presently within the oversight remit of the IGIS).

92. The Law Council considers that the proposed SCI-Act MA regime should be subject to equivalent oversight to that presently performed by the IGIS in relation to the ISA-MA regime. As noted below in relation to oversight, this will likely require the allocation of additional resources to the Commonwealth Ombudsman.

Revocation and cessation obligations

93. It is positive that there are express obligations under new sections 35AH and 35BA on the Minister to revoke an SCI-Act MA, and the Secretary to revoke intervention requests given to ASD under such an MA, if satisfied that the issuing grounds are no longer met.

94. However, the Law Council has identified the following apparent gaps in these obligations, which it recommends should be addressed before a Bill is introduced to Parliament:

- there is no obligation on the Secretary to inform the Minister (and the Director-General of ASD) as soon as possible if they become aware of facts to suggest that the issuing grounds are no longer met;

- there is no obligation on the Secretary or Director-General of ASD to cease taking action under an SCI-Act MA, or request issued under such an MA, if satisfied that the grounds no longer exist (even if the instrument has not yet been revoked);

- there is no obligation on the Secretary or Minister to cause ASD to be notified, as soon as possible, of the revocation of an SCI-Act MA (only the relevant owners or operators of the critical infrastructure asset and the IGIS). There is only an obligation to notify ASD of the revocation of an intervention request given by the Secretary under an SCI-Act MA; and

- given that an SCI-Act MA enlivens significant immunities from legal liability, the maximum timeframe of 48 hours for notifying the revocation of an SCI-Act MA and the revocation of an intervention request is too long. This should be shortened to one-to-two hours (even a longer timeframe is permitted for subsequently furnishing a written instrument or record of the revocation).

Recommendation 10—enhanced obligations concerning revocation/cessation

- **The revocation provisions in proposed section 35AH (SCI-Act MAs) and 35BA (Secretary's intervention requests under SCI-Act MAs) should be amended to address the matters identified at paragraph [94] of this submission.**

Involvement of the Australian Signals Directorate

Safeguards in relation to intervention powers

95. The Law Council recommends that the ED Bill is amended to include several additional safeguards in relation to the performance by ASD of functions under intervention requests given by the Secretary, pursuant to an SCI-Act MA. These measures are as follows:

- ***Conditions for executing an intervention request:*** when ASD is issued with an intervention request by the Secretary, under the purported authority of an SCI-Act MA, the Director-General of ASD should be subject to an express requirement to independently consider whether the actions requested are:

  - necessary, reasonable and proportionate; and

  - within the scope of authority of the underlying SCI-Act MA;

  If the Director-General of ASD is not reasonably satisfied of these matters, they must not do the acts specified in the request, and must inform the Secretary as soon as possible (who must then revoke or vary the direction, if this is possible to cure the defects identified by ASD);

- ***Additional requirements concerning the removal of computers from private premises:*** When ASD exercises powers of entry to private premises and removes computers, it should be subject to additional requirements to:

  - provide the occupant, owner and operator with a written receipt of the removal, which includes a statement of their rights to complain to the IGIS or Ombudsman (or both) and the process available to them for requesting return;

  - return the computer within a specified timeframe (for example, 24 hours) unless exceptional circumstances apply, in which case it may be extended incrementally, rather than the nebulous requirement of 'as soon as practicable'; and

- notify the IGIS of the removal and return, and additionally if ASD causes any damage to the computer during its removal; and

- ***Reporting requirements:*** ASD's reporting requirements to the Defence and Home Affairs Minister on its intervention activities in proposed section 35BH should be improved as follows:

  - the reporting deadline should be limited to seven days after the request, not three months as is proposed. It should be noted that, while MAs issued under the ISA are subject to a three-month statutory reporting timeframe, ISA- MAs:

    - are in force for a much longer period (up to six months, not 20 days); and

    - cover far broader activities (namely, the undertaking of a series of activities to produce intelligence for a specified purpose consistent with the agency's statutory functions; not responding to a particular cyber security incident to manage the impacts on a particular primary critical infrastructure asset); and

  - the reports should be required to include details of any removal of computers, and the doing of any act that caused, or was assessed as reasonably likely to cause, material loss, damage or interference to third parties who use or are reliant on that computer.

Recommendation 11—stronger safeguards in relation to ASD intervention

- **ASD's intervention powers under proposed Division 5 of new Part 3A of the SCI Act should be amended to include the safeguards listed at paragraph [95] of this submission.**

IGIS evidentiary certification function

96. Proposed section 35BG of the SCI Act purports to confer a general evidentiary certification function on the IGIS, to issue prima facie certificates in relation to 'any facts the Inspector-General of Intelligence and Security considers relevant with respect to anything done, or omitted to be done' by ASD or a staff member of ASD in the exercise of the powers of intervention, under a request given pursuant to an SCI-Act MA.

Absence of justification for an evidentiary certificate regime

97. The breadth of the proposed evidentiary certification function is extraordinary. No explanation appears to have been given in the Explanatory Document for **any** evidentiary certification function, let alone one that extends to **any matter** in respect of ASD's actions under the proposed intervention regime. In particular, no explanation is given as to why parties should not simply adduce evidence in accordance with the usual rules of evidence, with matters of admissibility and weight to be determined by the court in which legal proceedings are conducted.

Proposed conferral of an unlimited evidentiary certification function on the IGIS

98. Even more extraordinary is the proposal to confer an unlimited evidentiary certification function on the IGIS, rather than the Director-General of ASD (as is the

case with evidentiary certification functions under the ASIO Act about operational matters, which are conferred on the Director-General of Security).[10]

99. This creates a significant risk of the IGIS being exposed to pressure or influence by the Government of the day, or agencies or policy Departments, to issue certificates in proceedings challenging aspects of intervention powers exercised by ASD.

Significant differences to the IGIS's evidentiary certification functions under the ISA and Criminal Code

100. The proposed evidentiary certification function in new section 35BG of the SCI Act is distinguishable to the far more limited certification functions under section 14 of the ISA and Division 476 of the Criminal Code.

101. Under those provisions of the ISA and Criminal Code, ASD (among other intelligence agencies) is conferred with an immunity for acts done in the 'proper performance' of its statutory functions. The IGIS may issue a prima facie evidentiary certificate, at their discretion, in relation to whether an act was done in the 'proper performance' by ASD of its functions. This is the **only matter** that the IGIS may certify under the ISA and Criminal Code. This matter is connected explicitly with the elements of the immunities conferred on ASD (and other intelligence agencies). It is also connected explicitly with the IGIS's statutory function under the IGIS Act to conduct oversight of the propriety of intelligence agencies' activities (in addition to examining matters of legality and human rights compliance).

102. In sharp contrast, the proposed evidentiary certification function in new section 35BG of the SCI Act is not only unlimited, but it also has no nexus with the elements of the immunity in proposed section 35BF, or the specific oversight functions of the IGIS under the IGIS Act. As discussed below in relation to immunities, proposed section 35BF has a far broader scope than the immunities conferred on ASD under the ISA and Criminal Code, in that:

- there is no limitation to acts done in the 'proper performance' of ASD's functions; and
- the proposed immunity in new section 35BF also extends to acts done in the **purported exercise** of authority, not merely those acts that were, in fact, within the scope of legal authority.

103. There Law Council considers that there is a serious question as to whether it is appropriate for **any entity**, let alone an independent oversight body such as the IGIS, to have evidentiary certification functions as to whether ASD **purported to act** in compliance with the limits of its authority under proposed Part 3A of the SCI Act.

104. As discussed below in relation to immunities, the Law Council also recommends that the proposed immunity should be limited to acts done in **actual compliance** with authority, not purported compliance that was, in fact, non-compliant.

Recommendation 12—IGIS evidentiary certification function

- **Proposed section 35BG of the SCI Act should be amended to limit the evidentiary certification function of the IGIS to the matter of whether the actions taken by an ASD staff member were done in the proper**

[10] See, for example: ASIO Act subsections 21A(8) and (9) (Director-General may issue evidentiary certificates in relation to ASIO's power to confer immunities on persons who render voluntary assistance); and section 34AA (Director-General may issue evidentiary certificates in relation to ASIO's special powers warrants). See also, section 35R (Attorney-General may issue evidentiary certificates relating to the granting of special intelligence operation authorities).

performance by ASD of its functions, consistent with the scope of the evidentiary certification functions of the IGIS under section 14 of the ISA and Division 476 of the Criminal Code. This amendment should be contingent on amendments to the immunity in proposed section 35BF, to limit it to acts done in the proper performance of ASD's functions.

- **The admission and treatment of evidence of any other matters relating to ASD's actions should be left to the discretion of the court in the relevant legal proceedings.**
- **However, if there is no appetite to amend the immunity in section 35BF as recommended above, the evidentiary certification function in proposed section 35BG should be omitted from the Bill.**

Enforcement powers

105. The Law Council notes that the proposed enlivenment of regulatory powers under the RPA will have a significant effect on the rights and liberties of affected individuals. This effect will be particularly significant in relation to powers of monitoring and investigation, which enable entry to premises, the use of force against things, and the securing and seizure of items.

106. These powers are high-risk when conferred on any entity. The fact that the Department of Home Affairs (apart from the Australian Border Force) is a primarily a policy department, rather than an experienced regulator, heightens this risk.

107. Powers of enforcement are conferred on the Secretary and are delegable to any SES employee in the Department (irrespective of qualifications, skills and training). The Bill, in new subsections 49(2) and (3) of the SCI Act, further proposes to make these enforcement powers delegable to the heads and SES staff of 'relevant Commonwealth regulators' (being any Department or body specified in rules made by the Minister, without any statutory limitations on the power to prescribe entities).

108. If these powers are to be conferred, the Law Council considers that further information is required in relation to their need, as well as limitations on the persons who may exercise them, by reference to their qualifications, skills and training.

109. The proposed expansion of regulatory enforcement powers also increases the need for ongoing inspection by the Commonwealth Ombudsman of the Department's activities in training persons to exercise those powers, and in their execution.

110. The Law Council also strongly supports the application of the Australian Government Regulator Performance Framework to the Department in respect of the expanded regulatory powers under the SCI Act. That framework would require the Department to measure and evaluate its performance against several key performance indicators, and publish periodic reports on that performance. The Law Council is concerned that the Explanatory Document makes no mention of the intended application of this important evaluative and accountability mechanism (or any reasons for any suggestion that the Department should be exempt).

Recommendation 13—expansion of regulatory enforcement powers

- **Further explanation is required for the need to confer monitoring and enforcement powers in relation to the SCI Act, to enable Parliamentary and public scrutiny of the stated case.**
- **If those powers are to be conferred, there should be:**
  - **further conditions on the appointment of authorised officers, who are eligible to exercise those powers, by reference to their completion of specified training, and their possession of specified skills and qualifications; and**
  - **provision for the Commonwealth Ombudsman to perform a statutory inspection function in relation to this aspect of the Department's administration of the enforcement regime (particularly in relation to the training and appointment of authorised officers, and their exercise of intrusive powers);**
  - **limitations placed on the legislative powers delegated to the Minister to make rules prescribing a department or other body as a 'relevant Commonwealth regulator' for the purpose of the SCI Act. The Minister should not be permitted to prescribe an entity unless:**
    - **that entity is invested with regulatory functions under another law of the Commonwealth or a State or Territory, in relation to the applicable class of critical infrastructure asset;**
    - **the Minister is satisfied, on reasonable grounds, that the entity has appropriately skilled and trained personnel; adequate resources; rigorous governance, assurance, accountability and oversight mechanisms to exercise the regulatory powers; and a sound record of human rights compliance; and**
    - **the Minister has consulted the chief executive of the entity about a proposal to prescribe the entity being prescribed as a 'relevant Commonwealth regulator', and the chief executive has consented to this; and**
  - **a requirement that the Department is subject to the Australian Government Regulator Performance Framework.**

Independent review and oversight arrangements

111. While the ED Bill proposes some oversight-related measures, such as requirements for the IGIS to be given notification of certain matters, the Law Council is concerned that inadequate provisions is made for independent oversight and review of the operation of the expanded SCI regime.

112. Independent review and oversight are critical to public trust and confidence in the regime, having regard to its significant regulatory impost and the conferral of significant coercive powers. Independent review and oversight will demonstrably facilitate its lawful and proper operation.

Overarching issue: impact of secrecy provisions on review and oversight

113. The Law Council is concerned that the existing secrecy provisions of the SCI Act will be a major impediment to the effective exercise of review rights and oversight functions in respect of the expanded SCI regime.

- **section 45 of the SCI Act** prohibits the disclosure of 'protected information' (essentially, all information obtained under the SCI Act. The definition of 'protected information' is proposed to be expanded to cover information obtained under the new powers in the ED Bill); and
- **section 46 of the SCI Act** contains various exceptions, including for the purposes authorised or required under a law of the Commonwealth or a law of a State or Territory, if prescribed by rules. However, this is qualified by **section 47**, which provides that, except where necessary to do so for the purpose of giving effect to the SCI Act, an entity cannot be compelled to produce protected information to a court, a tribunal or any other person who has the power to require the production of information or documents (which would include the Ombudsman and IGIS, among other oversight bodies).

114. Accordingly, the SCI Act does not provide a clear legal pathway for voluntary disclosure to oversight bodies. In contrast, sections 42 and 43 contain express exceptions for disclosures to certain Ministers and their departments (including for the purpose of industry regulation or oversight) and law enforcement. Moreover, to the extent that an oversight body sought to use its statutory powers to compel the production of that information, section 47 would purport to override those powers.

115. In addition, the SCI Act makes no provision for disclosures to lawyers for the purpose of obtaining legal advice, or disclosures for the purpose of legal proceedings. On the contrary, section 47 expressly purports to override the powers of a court to compel production. It is not clear that the expression in section 47 'except where it is necessary to do so for giving effect to this Act' would cover the interests of a regulated entity in commencing proceedings to challenge a decision made under the SCI Act.

116. The secrecy provisions in existing sections 45-47 of the SCI Act therefore create a significant risk of frustrating the effective exercise of legal review rights and the performance of independent oversight functions in respect of the proposed regime.

117. The Law Council considers it essential that the overbreadth in these secrecy provisions is addressed, especially if the proposed amendments are to proceed. Otherwise the existing and expanded regime will be effectively unreviewable and will not be subject to meaningful and effective oversight.

Recommendation 14—expansion of permitted disclosures, and preservation of compulsory information-gathering powers of oversight and review bodies

- **Sections 45-47 of the SCI Act should be amended to provide that:**
  - **the SCI Act does not override the powers of courts, tribunals and oversight bodies to require the disclosure of protected information;**
  - **voluntary disclosures to the Commonwealth Ombudsman, IGIS and Australian Information Commissioner are permitted, for the purpose of those agencies performing functions or exercising powers in relation to the oversight of the SCI regime; and**
  - **voluntary disclosures are permitted for the purpose of:**

- **obtaining legal advice about an entity's obligations under, or in relation to, the SCI Act;**
- **commencing or responding to legal proceedings (in any Australian court, or in the Administrative Appeals Tribunal) under or in relation to that Act.**

Limitations in judicial review rights

118. Item 1 of Schedule 1 to the ED Bill proposes to amend the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (**ADJR Act**) to exclude from statutory judicial review all administrative decisions made under the proposed SCI-Act MA regime in new Part 3A of the SCI Act.

119. This exclusion will cover both the decisions of the Minister in relation to the issuing of MAs, and decisions of the Secretary in exercising powers under those MAs to issue directions to regulated entities and require ASD to undertake intervention action. (By extension, the Secretary also exercises an effective power to confer an immunity on ASD and thereby extinguish individuals' rights to legal remedies, by making an intervention request that enlivens the immunity for ASD personnel in proposed section 35BF of the SCI Act.)

120. The Explanatory Document states that the exclusion of ADJR Act review is considered 'entirely reasonable' on the basis of national security and the circumstances of urgency in which SCI-Act MAs are intended to be issued. It notes that judicial review remains under available under the original jurisdiction of the High Court and the mirroring jurisdiction of the Federal Court in section 39B of the *Judiciary Act 1903* (Cth).[11]

National security as the basis for a wholesale exclusion of ADJR Act review

121. The Law Council considers that a general appeal to national security is an inadequate justification for a **wholesale exclusion** of statutory judicial review rights, in respect of decisions to impose liabilities and take other actions that may have significant, adverse impacts on regulated entities and third parties that rely on the relevant critical infrastructure assets.

122. In particular, the stated justification does not explain why less restrictive alternatives to a wholesale exclusion could not be pursued. They include the deferral of the exercise of review rights until after the incident has been managed or the immediate risk has otherwise abated, rather than permanent extinguishment of those rights. Precedent for deferred exercise already exists in sections 9A and 9B of the ADJR Act in respect of decisions relating to criminal justice or civil proceedings. Other alternatives to wholesale exclusion include limiting the matters to be included in statutory reasons required to be given under section 13 of the ADJR Act.

123. Further, the stated justification does not explain why there must be a wholesale exclusion of **all decisions** made under new Division 3A, and not only the Minister's assessment that there is a risk of serious prejudice to security, defence or social or economic security, which is the focus of the justification advanced in the Explanatory Document.[12] This is not the only decision that must be made under Division 3A. The Minister must also assess a range of other matters in determining whether to issue an MA and the matters to be authorised, and the Secretary must also assess various matters in determining whether to exercise a coercive power under an MA.

[11] Explanatory Document, 65 at [418]-[419], and 66 at [422].
[12] Ibid, 65 at [419].

124. In the absence of any such justification and the gravity of the powers proposed to be conferred under new Division 3A, the Law Council recommends that a more nuanced approach is taken (as outlined in the recommendation below).

ADJR Act review as a perceived disincentive to industry cooperation

125. In addition, the Law Council does not agree with a further suggestion in the Explanatory Document that the availability of ADJR Act review rights will create a disincentive to industry cooperation, because it may require the compulsory disclosure of sensitive information to a court, and that this potential disincentive requires the exclusion of ADJR Act review.[13] In particular:

- existing section 47 of the SCI Act purports to override the powers of the courts to compel discovery; and
- further, even if section 47 is amended as recommended by the Law Council:
  - to the extent that a regulated entity may wish to commence judicial review proceedings in relation to a decision of the Minister or Secretary (or delegate) under new Part 3A, that entity will be in a position to individually assess the risks of disclosing its commercially or otherwise sensitive information in those proceedings, and determine whether those risks can be mitigated with applications for suppression or non-publication orders, or whether it would be preferable not to commence proceedings in order to avoid any disclosure of that information;
  - to the extent that an entity's information may be disclosed in proceedings to which it is **not** a party (or is not the applicant), the court's inherent powers to control its proceedings include powers to order suppression or non-publication of certain evidence, which provide mechanisms for protecting sensitive information; and
  - to the extent that the Commonwealth, as respondent, is concerned about the disclosure of sensitive information, it could claim public interest immunity. The Attorney-General could also seek to invoke the protective provisions of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).

Recommendation 15—statutory judicial review rights

- **Item 1 of Schedule 1 to the ED Bill should be omitted. Consideration should be given to making provision for the following matters:**
  - **the deferred exercise, rather than absolute extinguishment of, statutory judicial review rights;**
  - **the conferral of judicial review rights in relation to the administrative decisions and conduct of the Secretary in giving directions and issuing intervention requests under SCI-Act MAs (even if there is an exclusion or limitation on the review of the Minister's issuing decisions); and**
  - **more targeted limitations or exclusions on rights to review of Ministerial decisions, rather than wholesale exclusion.**

    In particular, while the Minister's decision-making about the existence of a threat to Australia's national security, defence or social or economic security might be excluded from review,

[13] Ibid, 65-66 at [420].

statutory judicial review rights could be conferred in relation to the Minister's assessment of the following statutory conditions:

- **technical feasibility of an authorisation for action or intervention directions;**
- **the fact that the relevant owners or operators of the critical infrastructure assets were 'unwilling or unable' to take action of their own volition to respond to the incident; and**
- **the basis for the Minister's satisfaction that authorising the Secretary to issue information-gathering directions is 'likely to facilitate a practical and effective response to the incident'.**

Absence of merits review rights

126. The Law Council also notes that no merits review rights are conferred in respect of decisions made under the proposed expansions to the SCI Act regime. The Law Council recommends that this is reconsidered in view of the following:

- the proposed exclusion of statutory judicial review rights, combined with the limitations in the utility and exercise of judicial review rights in original jurisdiction;
- the significance of the regulatory obligations imposed under the scheme (including liabilities to significant civil penalties and enforcement powers), and the breadth of discretion in imposing those requirements (including making assessments about matters that will necessarily require detailed knowledge and understanding of the operating systems, processes and methods of particular sectors and particular assets);
- the absence of in-built dispute resolution mechanisms in the ED Bill about decisions to issue directions under the new aspects of the SCI regime;
- the facilities available in the Security Division of the Administrative Appeals Tribunal to hear classified evidence, including its existing jurisdiction with respect to the review of ASIO security assessments underpinning Ministerial directions given under existing section 32 of the SCI Act; and
- the importance of independent, fair and transparent review rights to industry and public trust and confidence in the operation of the proposed regime, including by ensuring that Commonwealth officials exercising the significant powers proposed under the regime are subject to rigorous accountability mechanisms.

Recommendation 16—merits review rights

- **The ED Bill should be amended to confer merits review rights in respect of the decisions of the Minister and Secretary (or delegates) under all of the proposed expansions of the SCI regime.**

Independent operational oversight

Commonwealth Ombudsman

127. The ED Bill proposes to confer significant new and expanded powers on the Secretary of the Department of Home Affairs. Extraordinary powers must be accompanied by commensurate oversight measures. The ED Bill does not propose

to confer additional functions on the Commonwealth Ombudsman to conduct inspections of the activities of the Department under the expanded SCI regime.

Inspection function

128. Unlike the statutory functions of the IGIS under the IGIS Act, the Commonwealth Ombudsman does not have standing jurisdiction under the Ombudsman Act to conduct inspections of agencies' activities. Rather, inspection functions must be conferred under individual statutes, as is the case under the TIA Act and Telco Act.

129. While the Ombudsman would have functions under the Ombudsman Act to investigate complaints or initiate own-motion investigations into matters of administration arising from the operation of the SCI Act (as amended), the Law Council considers that a standing inspection function is needed.

130. A standing inspection function, equivalent to that of the IGIS in relation to ASD's activities under proposed Division 3A or otherwise in support of the SCI regime, would enable the Ombudsman to undertake to enable periodic monitoring of the Department's activities, rather than investigating specific incidents.

131. This is important given that investigations are normally commenced 'for cause' where there is a credible suspicion of wrongdoing (commensurate with the significance of the powers of investigation). In contrast, ongoing inspections can assist in the early identification of issues, and enable the oversight body to work with the relevant agency to develop and implement corrective actions, before there is a need for major remedial action. Standing inspection functions can also provide assurance to the public and regulated entities that there is regular oversight, and not merely investigations when a potential problem is identified.

Resourcing

132. In view of previous comments of the Commonwealth Ombudsman about the need for further resources to perform additional oversight functions under new or expanded national security laws, the Law Council urges the Government to increase the Ombudsman's resourcing to enable effective oversight of the expanded SCI regime. This should include adequate resources to ensure an appropriate number of staff to perform oversight functions, access to technical expertise (especially in conducting oversight of decision-making about whether a proposed direction or requirement is technically feasible), and access to security related infrastructure (such as premises, ICT systems and security cleared staff).

Secrecy provisions

133. As mentioned above, the Law Council is also concerned that the secrecy provisions of the SCI Act purport to prohibit voluntary disclosures of 'protected information' to the Ombudsman (potentially including as part of complaints made by the owners or operators of critical infrastructure assets, or affected third parties that rely on those assets) as well as purporting to override the Ombudsman's coercive information-gathering powers in investigations (or inspections, if such a function were conferred under the SCI Act).

134. In addition, while proposed section 43A of the SCI Act permits Ombudsman officials to disclose protected information to IGIS officials, the Law Council is concerned that no consequential amendments are proposed to the secrecy and non-disclosure provisions of the Ombudsman Act. This may mean that the intended information-sharing arrangements under the SCI Act will not be legally effective.

Attorney-General's certification power

135. Further, unlike the IGIS, the Commonwealth Ombudsman is subject to Ministerial intervention in relation to their acquisition of information. Subsection 9(3) of the Ombudsman Act provides that the Attorney-General can issue a certificate to the Commonwealth Ombudsman in respect of certain information, which has the effect of prohibiting the Ombudsman from requesting or requiring another person to disclose it. The Attorney-General can issue a certificate on various grounds, including if satisfied that the disclosure of the specified information would be likely to prejudice security.

136. The Law Council queries the appropriateness of such intervention powers in respect of the SCI regime, given that this regime will necessarily be focused on national security and will conceivably deal with classified and otherwise sensitive information relevant to Australia's national security, defence and international relations.

Recommendation 17— Commonwealth Ombudsman

- **The Commonwealth Ombudsman should be conferred with ongoing statutory inspection functions in relation to the administration by the Department of Home Affairs of the expanded SCI regime, in particular the issuing of binding directions to regulated entities, and its applications for, and execution of, SCI-Act MAs.**
- **Resourcing for the Commonwealth Ombudsman should be increased to enable the performance of these oversight functions, including:**
  - **access to independent technical expertise;**
  - **access to the necessary security infrastructure (including physical premises, ICT systems and security cleared staff).**
- **Consideration should be given to the adequacy of disclosure provisions under the *Ombudsman Act 1976* (Cth) to enable effective oversight of the SCI regime. This should include consideration of:**
  - **provisions governing voluntary and compulsory disclosures of information to, and by, Ombudsman officials, in relation to 'protected information' under the SCI Act; and**
  - **the appropriateness of the Attorney-General's certificate provisions in subsection 9(3) in relation to their potential application to 'protected information' under the SCI Act. (Noting that the issuance of a certificate under the Ombudsman Act prevents the Ombudsman from obtaining information of matters on specified grounds, including national security—which is the focus of the SCI regime.)**

Australian Information Commissioner

137. The SCI regime enables the collection of personal information (although some of the proposed cyber security notification obligations expressly prohibit the collection of personal information). Further to the Law Council's comments on privacy matters associated with the SCI regime in its submissions on the Security of Critical Infrastructure Bill 2017,[14] the Law Council is concerned to ensure that there are

[14] Law Council of Australia, *Submission to the PJCIS Review of the Security of Critical Infrastructure Bill 2017*, (February 2018), 3-4 at [18]-[23].

adequate compliance oversight mechanisms in relation to the obligations of the Department under the *Privacy Act 1988* (Cth) (**Privacy Act**).

138. Presently, the secrecy provisions of the SCI Act may restrict the ability of the Australian Information Commissioner from performing their oversight functions, as Privacy Commissioner, under the Privacy Act.

139. The Law Council recommends the Government, in consultation with the Australian Information Commissioner, considers whether consequential amendments are needed to the secrecy provisions of the SCI Act, and the *Australian Information Commissioner Act 2010* (Cth) or the Privacy Act (or all of these enactments) to ensure that there is effective, independent compliance oversight, including an avenue for complaints of alleged breaches to be investigated and for privacy assessments to be conducted, and enforcement powers under the Privacy Act to be exercised as required.

Recommendation 18—Australian Information Commissioner

- **Consideration should be given to whether the Australian Information Commissioner requires access to 'protected information' under the SCI Act for the purpose of performing their oversight functions in relation to information obtained and handled under the SCI regime, particularly in performing their functions as Privacy Commissioner.**
- **The Australian Information Commissioner should be consulted on this matter, if this has not already occurred in the development of the ED Bill. The Explanatory Memorandum to the Bill (once introduced) should document the fact of consultation, whether the approach proposed in the Bill accords with the Information Commissioner's advice, and the reasons for any departure from that advice.**

Inspector-General of Intelligence and Security

140. While the ED Bill contains a number of measures that will assist the IGIS in exercising their oversight functions and powers in relation to ASD (including notification requirements in relation to SCI-Act MAs, and a power to share information with the Commonwealth Ombudsman) the Law Council is concerned that the proposed amendments do not go far enough in respect of the following:

- **secrecy provisions in the SCI Act**: as noted above, section 47 of the SCI Act purports to override the compulsory powers of the IGIS to obtain information as part of inquiries. The absence of an express permission in the SCI Act for people to make disclosures to IGIS officials also calls into question the relationship of the immunity in section 34B of the IGIS Act for all disclosures made to the IGIS in connection with their oversight functions with the prohibition on disclosures (and the associated offence for breach) in the SCI Act. It would be preferable for the two statutes to make express provision for their interaction, namely by amending the SCI Act to include an exception for disclosures to IGIS officials; and
- **secrecy provisions in the IGIS Act:** while the SCI Act purports to allow IGIS officials to disclose 'protected information' under that Act to Ombudsman officials, this does not overcome the prohibitions on disclosure under the IGIS Act and will therefore be ineffective to enable the intended information-sharing to occur. Section 34 of the IGIS Act relevantly prohibits IGIS officials from disclosing information obtained in the performance of their oversight functions under the IGIS Act, except for the purpose of performing functions under that Act. Consequential amendments to the IGIS Act are therefore needed.

141. In addition, the introduction of an MA regime under the SCI Act, which confers powers on the Minister for Home Affairs and the Secretary of the Department to require ASD to undertake acts of intervention, raises a significant question about the possible fragmentation of oversight. Just as the ED Bill proposes greater, and novel, interoperability between Home Affairs and ASD, interoperability of applicable oversight must also be factored into the design of the regime. It should not be dealt with as an 'add on' after the core parameters for the exercise of powers are set.

142. To this end, the Law Council queries whether the functions of the IGIS should be extended consequentially as part of the proposed SCI reforms to include oversight of the functions of the Department of Home Affairs under new Part 3A of the SCI Act.

143. Alternatively, this issue should be considered as part of the forthcoming legislative amendments to implement the Government's acceptance of the recommendations of the *2017 Independent Intelligence Review*, to expand the oversight functions of the IGIS to cover the intelligence functions of the Department of Home Affairs, the Australian Federal Police, the Australian Criminal Intelligence Commission and AUSTRAC.

Recommendation 19—Inspector-General of Intelligence and Security

- **Section 34 of the IGIS Act should be amended consequentially to enable IGIS officials to disclose 'protected information' under the SCI Act to the Commonwealth Ombudsman. This will remove the conflict between the prohibition on such disclosure in section 34 of the IGIS Act and the permitted disclosure in proposed section 43B of the SCI Act (item 50 of Schedule 1 to the ED Bill).**
- **Further consideration should be given to oversight arrangements for the proposed intervention regime in new Part 3A of the SCI Act. In particular, consideration should be given to the following:**
  - **expanding the oversight functions of the IGIS to cover the actions of the Secretary of the Department of Home Affairs in relation to the SCI-Act MA regime (that is, the Secretary's functions in requesting and executing MAs, and making subsequent use or disclosures of information obtained); or**
  - **in developing legislation to implement the Government's acceptance of the recommendations of the *2017 Independent Intelligence Review* to expand the jurisdiction of the IGIS to include oversight of the intelligence functions of the Department of Home Affairs, consideration should be given to the arrangements for the oversight of the Department's functions under the SCI-Act MA regime. In particular, consideration should be given to the need for comprehensive and coordinated oversight with respect to the interoperability of the Department and ASD under that regime.**

Parliamentary and independent review of the expanded SCI regime

Parliamentary review

144. Existing section 60A of the SCI Act requires the PJCIS to undertake a statutory review of the operation of the SCI regime, which must commence in 2021. This provision was inserted via Parliamentary amendments to the originating Bill to implement a recommendation of PJCIS for such review. That recommendation was

made in recognition of the novel nature of the regulatory regime, and its potentially significant impacts on industry, and on rights and liberties more generally.[15]

145. However, the ED Bill does not propose to update section 60A of the SCI Act to make provision for a statutory review of the expanded SCI regime after the proposed amendments have been operational for a reasonable period of time (for example, in the range of three years).

146. The Law Council supports the routine use of statutory provisions requiring the parliamentary or independent review of legislation after sufficient experience has been accumulated in its practical operation or administration.[16] It would be preferable if such review provisions were routinely included in proposed legislation on a pro-active basis, rather than being included only on the recommendations of Parliamentary Committees. Accordingly, the Law Council recommends that the Bill is amended to make provision for a further statutory review of the expanded regime.

147. Ideally, this would be performed by the PJCIS. However, given that Committee's significant workload and the technical issues raised by the proposed expansion of the SCI regime, consideration could given to appointing an independent expert to conduct a statutory review, or conferring a function on the INSLM. The PJCIS could then use that report as the basis for its subsequent parliamentary review.

Recommendation 20— independent review of the expanded SCI regime

- **The Bill should provide for further statutory reviews of the expanded SCI regime after three years of operation, as follows:**
  - **an independent review to be undertaken by either the INSLM, or an eminent person with expertise in regulation and enforcement matters in relation to critical infrastructure, who is appointed by the Government with the prior agreement of the Opposition; and**
  - **a subsequent review by the PJCIS, taking into account the findings of the abovementioned independent review.**

Performance auditing

148. In addition, given the proposed significant expansion of the regulatory and administrative functions of the Department in relation to the expanded SCI regime, the Law Council considers that there would be merit in the Commonwealth Auditor-General conducting a performance audit of the Department's activities.

149. While the determination of audit priorities is an independent decision for the Auditor-General, it would be open to the Department to suggest that the Auditor-General consider including this matter in their future audit priorities (noting that the Auditor-General periodically invites suggestions about audit priorities).

150. A suggestion of this kind directly from the Department would be a tangible and powerful demonstration of its stated commitment to effective regulatory performance, given that a performance audit would provide a valuable opportunity

[15] PJCIS, *Report on the Review of the Security of Critical Infrastructure Bill 2017*, (March 2018), rec 9.

[16] See further: Department of the Prime Minister and Cabinet, *Legislation Handbook*, (February 2017), 26 at [5.26] which states that, 'in developing new legislation and amending existing legislation, departments will need to consider whether a mechanism for reviewing the legislation could be included'. The Handbook directs departments responsible for developing legislative amendments to consider whether such a review should be one-off or regular/periodic, and to specify the matters that should be considered. It gives examples, including whether the legislation is operating effectively, has resulted in unintended consequences, remains relevant and clear or contains any outdated or redundant provisions.

for independent evaluation, subject to the statutory procedural fairness obligations and protections for sensitive information under the *Auditor-General Act 1997* (Cth). Independent evaluation by the Auditor-General could usefully facilitate continuous improvement in the performance of regulatory and other administrative functions.

151. The Law Council also encourages the Government to consider increasing the budget of the Australian National Audit Office to facilitate performance auditing of the operation of major recent and proposed expansions to national security legislation, including the proposed expansions of the SCI regime.

Recommendation 21—suggested performance audit priority

- **The Government should suggest a performance audit priority to the Commonwealth Auditor-General in relation to the expanded regulatory regime. Namely, the performance by the Department of Home Affairs in administering the SCI and TSSR regimes, focusing on that Department's performance as a regulator.**
- **The Australian National Audit Office should be resourced adequately to perform the suggested performance audit.**

Immunities from legal liability

152. The ED Bill proposes to confer complete immunities from criminal and civil liability on the following persons.

- the Director-General of ASD and staff members of that agency, in executing intervention directions issued by the Secretary of the Department, in relation to a serious cyber security incident (under the authority of an SCI-Act MA);[17] and
- constables assisting ASD in gaining entry to private premises in accordance with a direction in respect of a serious cyber security incident, which is given by the Secretary under the authority of an SCI-Act MA.[18]

153. The ED Bill further proposes to confer civil immunities from liability to damages on regulated entities (but not injunctions or non-pecuniary remedies), in respect of acts done in compliance with:

- directions given by the Secretary of the Department in relation to a serious cyber security incident;[19]
- directions given by the Minister under the existing power of direction in section 32 which requires a regulated entity to take, or refrain from taking, a specified action on security-related grounds (provided that ASIO has furnished a security assessment in relation to that entity);[20] and
- obligations to provide notification in relation to cyber security incidents.[21]

154. The Law Council acknowledges the desire to confer a degree of legal protection on the individuals who are required to perform functions, exercise powers or comply with non-discretionary obligations under the expanded SCI regime.

[17] ED Bill, Schedule 1, item 45 (inserting proposed section 35BF of the SCI Act).
[18] Ibid.
[19] Ibid (inserting proposed section 35AW of the SCI Act).
[20] Ibid, Schedule 1, item 44 (inserting proposed section 35AAB of the SCI Act).
[21] Ibid, Schedule 1, item 39 (inserting proposed section 30BE of the SCI Act).

155. The Law Council also supports the express limitation of the proposed civil immunities for regulated entities to liability in damages, thereby preserving the rights of affected individuals to seek and obtain non-pecuniary remedies, such as injunctions and declarations. This is consistent with previous recommendations of the Law Council in relation to civil immunities in other regulatory regimes, particularly the industry assistance regime in Part 15 of the Telco Act, which was enacted by the TOLA Act.

Less restrictive alternatives to civil immunities—statutory indemnification

156. However, the Law Council notes that no justification has been given for the proposed conferral of a **civil immunity**, as distinct to the conferral of a **statutory indemnity** by the Commonwealth in relation to civil liability incurred by ASD personnel, constables and regulated entities in performing the above functions.

157. An indemnity would be a less restrictive alternative to the complete extinguishment of rights to any legal remedies by persons who suffer loss or damage as a result of the activities of emanations of the state; and the extinguishment of legal rights to seek damages in respect of the acts of critical infrastructure owners or operators, which are done at the behest of the state under the SCI Act.

158. Given that a statutory indemnity would expose the Commonwealth to significant financial liability, it would also provide an extremely strong incentive for the reasonable and proportionate exercise of powers and performance of functions under the expanded regime, including facilitating the adoption of rigorous internal governance and assurance frameworks.

Immunities for ASD personnel

Scope of proposed section 35BF immunity

159. The Law Council notes that the proposed immunities in new section 35BF of the SCI Act cover acts done by ASD and constables in the good faith **'purported'** exercise of a power or authority under the intervention regime, in addition to acts that are within the actual scope of authority.

160. In contrast, the proposed civil immunities for damages for private owners and operators of critical infrastructure assets are limited expressly to acts done in compliance with the relevant regulatory obligations.

161. The Explanatory Document does not appear to address the reasons for the differential, and preferential, treatment of ASD (and constables assisting ASD) as compared to regulated entities that are required to comply with various directions under the expanded SCI regime.

162. In any event, the Law Council does not support the proposed extension of civil immunities to acts done by ASD (or constables assisting ASD) in **purported compliance** with the scope of a power or authority conferred on them under the SCI Act as amended. This may have the undesirable effect of immunising negligence as to whether an intended action was, in fact, within the scope of a statutory power, authority or function.

163. That is, a member of ASD (or a constable assisting ASD) may act in good faith, in that they had an honest belief that an intended act was within their legal authority, and they acted without malice or an improper ulterior purpose in carrying out that act. However, the person may nonetheless fail to discharge their civil duty of care to third parties that are affected by their actions, to make reasonable inquiries to ascertain the actual scope and limits of their legal authority to act.

164. Law Council considers that the immunity should not be available in such circumstances, and it should be limited expressly to acts that are done in **actual compliance** with the scope of authority conferred on ASD (or constables assisting).

165. If there is a desire to protect individuals who act pursuant to an authority conferred by an instrument that has been revoked or varied, and the individuals are not reckless about the revocation or variation, then the Bill should include an explicit provision which targets the immunity specifically to these circumstances. There is precedent for the use of such immunity in respect of ASIO's special intelligence operations,[22] and controlled operations conducted by law enforcement agencies.[23]

Conferral of multiple, inconsistent immunities on ASD

166. Moreover, the Law Council is concerned that the proposed immunity in favour of ASD personnel in section 35BF of the SCI Act is inconsistent with the scope of other immunities conferred by section 14 of the ISA and Part 10.7 of the Criminal Code (presently section 476.5, which is proposed to be renumbered by the ED Bill to new section 476.6).

167. The proposed immunity in new section 35BF of the SCI Act is not limited to acts done in the **proper performance** by ASD of its functions, and consequently, there is no specific evidentiary certification function conferred on the IGIS in relation to whether an act was done in the 'proper performance' of ASD's functions. (Rather, as noted above, the proposed evidentiary certification function in new section 35BG applies to 'any facts the Inspector-General … considers relevant' and this is not tied to the elements of an immunity provision. The Law Council has separately suggested the limitation of scope of that certification function in the discussion of the SCI-Act MA regime above).

168. The Law Council considers that the 'proper performance' of a function imports a higher standard than the 'good faith purported exercise of authority' (which is the threshold for the immunity in proposed section 35BF of the SCI Act).

169. Moreover, the immunity in proposed section 35BF of the SCI Act does not contain an equivalent requirement to that in proposed subsection 476.6(8) of the Criminal Code for ASD to notify the IGIS when it does an act that enlivens the immunity, which causes significant loss or damage to a third party. The Law Council considers that there is no reason for limiting the IGIS notification requirement to the immunity in the Criminal Code for computer-related acts that occurred in Australia but were, at the time of the act, intended to occur overseas, and were reasonably believed to have occurred overseas.

170. The inconsistency in the scope and notification requirements of the immunities will be particularly problematic if ASD is directed by the Secretary of the Department under proposed Part 3A of the SCI Act to intervene in a cyber security incident by causing a computer-related act to occur **outside Australia**.

171. In this case, the actions of the relevant ASD personnel could be potentially covered by both the immunity in proposed section 35BF of the SCI Act, and the immunity in proposed section 476.6 / existing section 476.5 of the Criminal Code.

Recommendation 22—safeguards in relation to proposed immunities

- **Consideration should be given to the Commonwealth indemnifying persons exercising powers, performing functions or duties, or**

[22] *Australian Security Intelligence Organisation Act 1979* (Cth), section 35M.

[23] *Crimes Act 1914* (Cth), section 15HD.

complying with regulatory requirements, under the expanded SCI regime, in preference to the conferral of a civil immunity, which extinguishes affected individuals' rights to legal remedies.

- **The proposed immunities in new section 35BF of the SCI Act should not cover the exercise of a power or authority by ASD (or constables assisting) in purported compliance with the scope of their authority. Rather, only actual compliance should attract immunity.**
- **The scope of the immunities available to ASD under proposed section 35BF of the SCI Act should be made consistent with those under proposed section 476.6 of the Criminal Code, in that the SCI Act immunity should:**
  - **apply to acts done in the proper performance by ASD of its intervention functions under new Division 3A of the SCI Act;**
  - **be subject to an evidentiary certification by the IGIS in relation to whether an action of an ASD staff member was undertaken in the 'proper performance' by ASD of its functions (and not the broader evidentiary certification function in proposed section 35BG in relation to any facts); and**
  - **impose statutory obligations on ASD to notify the IGIS if it undertakes acts that enliven the immunity, which are reasonably likely to cause material loss or damage to a third party, or material interference with, obstruction of or disruption to the lawful use of a computer in Australia.**
- **ASD's statutory reporting requirements under proposed section 35BH of the SCI Act should be expanded to provide details to the Minister for Defence and the Minister for Home Affairs of any reliance on the immunity in section 35BH, which caused, or was assessed as being likely to cause, material loss, damage or interference to third parties.**

Schedule 2: expanded immunities for the Australian Signals Directorate

172. Schedule 2 to the ED Bill proposes to expand the immunities conferred on ASD under Division 476 of the Criminal Code, in relation to the computer offences in Part 10.7 and any other offences under Commonwealth, State or Territory laws, and any civil liability for those acts.

173. This proposed expansion would be additional to the criminal and civil immunities proposed in new section 34BF of the SCI Act (per Schedule 1 to the ED Bill) in relation to the good faith exercise, or purported exercise, by ASD of the intervention powers under new Part 3A of the SCI Act, on the direction of the Secretary.

Current immunities for 'computer-related acts'

174. Presently, subsection 476.6(5) of the Criminal Code provides that ASD, ASIS and AGO are not subject to any civil or criminal liability for any 'computer-related act' that is done in the proper performance of a function of the agency. This is provided that one of the following circumstances exists:

- the act is done outside Australia;[24] or
- the act is done inside Australia, but it is preparatory or ancillary to the doing of another act outside Australia, and the act done inside Australia is not one for which ASIO would require a warrant or statutory authorisation (namely, telecommunications interception or telecommunications data access, or access to data held in, or accessible from, a computer).[25]

175. A 'computer-related act' means an act, event, circumstance or result involving:

(a) the reliability, security or operation of a computer; or

(b) access to, or modification of, data held in a computer or on a data storage device; or

(c) electronic communication to or from a computer; or

(d) the reliability, security or operation of any data held in or on a computer, computer disk, credit card, or other data storage device; or

(e) possession or control of data held in a computer or on a data storage device; or

(f) producing, supplying or obtaining data held in a computer or on a data storage device.[26]

176. The limitation of the immunity to acts done outside Australia (or preparatory or ancillary acts) reflects that the functions of ASIS, ASD and AGO are limited to the collection of intelligence in relation to the acts, capabilities and intentions of persons outside Australia. The IGIS has a function to issue an evidentiary certificate that an act was done in the proper performance by ASD, ASIS or AGO of its functions.[27]

Proposed expansions of the immunities

177. The key proposed amendments in Schedule 2 to the Bill will:

- expand the immunities to acts of ASD which cause a computer-related act to occur, not merely the direct doing of a computer related act;[28]
- expand the immunity for computer-related acts done outside Australia to include computer-related acts that are done inside Australia, but which ASD reasonably believed would occur outside Australia;[29]
- expand the immunity for preparatory and ancillary actions to those which are done outside Australia, as well as inside Australia (and in both cases, this immunity excludes acts for which ASIO would require a warrant or statutory authorisation to do in Australia, including telecommunications interception and telecommunications data access);[30] and
- oblige ASD to give the IGIS written notification of instances in which it has relied on a statutory immunity, if it is aware that the computer-related act has

[24] Criminal Code, subsection 476.5(1).
[25] Ibid, subsections 476.5(2) and (2A).
[26] Ibid, subsection 476.5(3).
[27] Ibid, subsections 476.5(2B) and (2C).
[28] Bill, Schedule 2, item 6 (inserting proposed subsections 476.6(1) and (2) of the Criminal Code).
[29] Ibid (inserting proposed subsection 476.1(1) of the Criminal Code).
[30] Ibid (inserting proposed subsections 476.6(2) and (3) of the Criminal Code).

caused material damage to, interference with, or obstruction of, a computer that is in Australia.[31]

Law Council position

178. Any proposal to confer immunities from legal liability on an emanation of the state is a highly significant measure. In addition to conflicting with the fundamental notion that the law should apply equally to all persons, the conferral of civil liability extinguishes the rights of aggrieved persons to legal remedies for loss, harm or damage suffered. A cautious approach is particularly important where it is intended that the relevant agency will operate on a largely (or entirely) covert basis to undertake the acts which are covered by the proposed immunity.

The need for the expanded immunity

179. The Law Council acknowledges the justification provided in the Explanatory Document, that it can be technically impossible for ASD to be certain that a computer-related act which is intended to be carried out overseas will, in fact, be carried out on a computer that is located outside Australia, and to exclude the possibility that one or more of the computers being targeted (or which may be affected collaterally) is, in fact, in Australia.[32]

180. The Law Council acknowledges that there are significant difficulties in identifying precisely the location of a computer, given global network connectivity; the use of geolocation blocking or obfuscation technologies by malicious actors; the portability of devices and infrastructure; and the fact that the definition of a 'computer' in many statutes, in fact, covers multiple individual devices (for example, one or more networks or systems, or any combination of these).

Expanded criminal immunity

181. No explanation is given as to why the existing defence of mistake of fact in section 9.1 of the Criminal Code (in relation to the reasonable belief that the relevant computer-related act would occur outside Australia) would not sufficiently address the identified risk that ASD staff members may be exposed to criminal liability.

182. Presumably, mistake of fact would be the present legal basis for any computer-related acts carried out by ASD which are directed to computers that are reasonably but mistakenly believed to be overseas.

183. Any private individual or body corporate would need to rely on the defence of mistake of fact in relation to applicable elements of the computer offences in Part 10.7 in relation to their activities, including actions to secure computer networks or systems utilised by critical infrastructure assets which they own, operate or use. The basis for conferring preferential treatment upon ASD has not been articulated.

Expanded civil immunity

184. No specific explanation is given for the expansion of civil immunity for computer-related acts done inside Australia, which were intended to occur overseas.

185. As noted above in relation to the proposed immunities in the SCI Act in Schedule 1 to the ED Bill, a civil immunity extinguishes the rights of affected individuals to legal remedies in respect of loss or damage sustained as a result of the disruption or disabling of the computers. This includes the extinguishment of a right to a legal

[31] Ibid (inserting proposed subsection 476.6(8) of the Criminal Code).

[32] Explanatory Document, 69 at [443]-[444].

remedy for so-called 'relational loss', such as adverse financial impacts on businesses which use those computers.

186. It does not follow that the justification for a criminal immunity must extend automatically to a civil immunity. The Law Council also cautions against any assumption that the conferral of a civil immunity is any less serious or significant than a criminal immunity. The extinguishment of a right to a legal remedy for serious loss, damage or harm can have a disastrous impact on the lives and livelihoods of the affected individuals, which will also have broader social and economic effects.

187. These cautions should be given particular weight when the act causing loss or damage is done inside Australia. This reflects that the ensuing harm will almost certainly be sustained by Australian people, whose security and wellbeing the Government and its security agencies are entrusted, and empowered, to protect.

Safeguards

188. If the proposed expansion of the immunity is proceeded with, it is essential that its scope is targeted precisely, and that it is made subject to strong oversight mechanisms, including reporting requirements.

189. The Law Council acknowledges that the proposed amendments make some credible attempts to satisfy this imperative, namely:

- the proposed expansion of the immunity to computer-related acts done in Australia in new subsection 476.6(1) will be subject to the same requirements as the existing immunity for computer-related acts done outside Australia. Namely, it will only apply to acts done in the **proper performance** by ASD of its functions, which will be subject to evidentiary certification by the IGIS;
- an additional obligation to notify the IGIS will apply to the expanded immunity (and the existing immunity for preparatory acts in Australia) if ASD becomes aware of a computer-related act causing material damage, interference or obstruction of a computer in Australia;
- in the case of computer related acts done, or intended to be done, outside Australia for the purpose of producing intelligence on an Australian person in accordance with an MA issued under section 9 of the ISA, the statutory issuing criteria of necessity and proportionality will apply under that provision; and
- in the case of computer-related acts done, or intended to be done, outside Australia pursuant to an intervention direction given under an SCI-Act MA (per proposed Part 3A of the SCI Act in Schedule 1 to the Bill), the statutory issuing criteria of necessity, proportionality and technical feasibility will apply.

190. However, the Law Council recommends some further amendments to deal with telecommunications interception and access to telecommunications data, and to address gaps in the proposed IGIS notification obligations.

Proposed scope of the expanded immunity

Ability to intercept telecommunications and access telecommunications data

191. The expanded immunity in proposed subsection 476.6(1) applies to conduct undertaken inside Australia, which ASD reasonably believes is likely to cause a computer-related act, event or circumstance to occur outside Australia.

192. The expanded immunity is **not** subject to the prohibition in proposed subsection 476.6(3) on intercepting telecommunications or accessing stored communications or

telecommunications data, or accessing data held in or from a computer. That prohibition applies only to the immunity in proposed subsection 476.6(2) for preparatory or ancillary acts done inside or outside Australia.

193. This means that, when ASD performs a function under the new MA regime in proposed Part 3A of the SCI Act—or when it performs one of its existing functions under section 7 of the ISA—its criminal and civil immunities are not contingent on it refraining from doing acts or things for which ASIO would need a warrant or a statutory authorisation to do in Australia. However, this is provided that ASD **reasonably believed** that the relevant computer-related act it has undertaken in accordance with an SCI-Act MA, or under the ISA (including under an MA where required) would occur **outside Australia**. It will not be relevant that the computer-related act, in fact, occurred inside Australia.

Overriding the existing statutory prohibitions under the TIA Act

194. Proposed subsection 476.6(4) states that the immunity provisions in proposed subsections 476.6(1) and (2) override all other Australian laws. Moreover, the criminal immunity provisions in subsections 476.6(1) and (2) are not limited to immunity from the computer offences in Part 10.7 of the Criminal Code, but rather are expressed as applying to any criminal liability under any law of Australia.[33]

195. Consequently, the expansion of immunity in proposed subsection 476.6(1) would override the prohibitions and associated offences in the TIA Act on intercepting and communicating the contents of telecommunications, and accessing and communicating stored communications and telecommunications data, other than in accordance with warrants or authorisations obtained under that Act. It would not merely override the computer offences in Part 10.7 of the Criminal Code.

New Part 3A of the SCI Act may lead to increased use of the s 476.6(1) immunity

196. It is conceivable that the proposed SCI-Act MA regime in new Part 3A of the SCI Act (per Schedule 1 to the ED Bill) will increase the circumstances in which ASD may seek to rely on the expanded immunity in proposed subsection 476.6(1) of the Criminal Code in relation to computer-related acts that it caused to occur inside Australia, but had reasonably believed would occur outside Australia. (This would be additional to the proposed immunity Schedule 1 to the ED Bill, in new section 34BF of the SCI Act, in relation to acts done in good faith in the exercise, or purported exercise, of intervention powers under the SCI Act.)

197. This reflects that the SCI-Act MA regime is a legal pathway for ASD to undertake a larger number of computer-related acts than may be presently possible for the purpose of protecting or defending critical infrastructure assets in Australia. In turn, this increases the possibility that the SCI-Act MA regime, in combination with the immunity provision in new subsection 476.6(1) of the Criminal Code, will increase the amount of 'incidental' or unintended telecommunications intercepts undertaken and telecommunications data accessed by ASD.

198. The Law Council acknowledges that proposed subsection 35AX(5) of the SCI Act (inserted by Schedule 1 to the ED Bill) provides that intervention requests issued in

[33] In addition to the words 'any civil or criminal liability' in the chapeau to each of proposed subsections 476.6(1) and (2) the expression 'criminal or civil liability' is defined in proposed subsection 476.6(10) to mean 'any civil or criminal liability (whether under this Part, under another law or otherwise)'. This is consistent wit the definitions and statutory expression in existing section 476.5 (which will apply only to ASIS and AGO under the proposed amendments, and new section 476.6 will deal exclusively with ASD).

accordance with an SCI-Act MA cannot authorise ASD to intercept telecommunications, or access stored communications or telecommunications data.

199. However, those prohibitions are limited to communications that are passing over, or have passed over, the Australian telecommunications network (**ATN**); or data pertaining to such communications. The issue is that the proposed immunity in new subsection 476.6(1) of the Criminal Code will apply if:

- ASD is lawfully requested, under an SCI-Act MA to cause a computer-related act to occur **outside Australia** (which might lawfully include the incidental interception of telecommunications that are passing over, or have passed over, a **foreign telecommunications network**, or accessing **foreign telecommunications data**); and
- ASD staff engage in conduct which causes a computer-related act to occur, with the intention and reasonable belief it will occur outside Australia; **but**
- the computer-related act ultimately occurs inside Australia; **and**
- the computer-related act causes the **unintentional** interception of a telecommunication that is passing over the ATN, or access to a stored communication that has passed over the ATN, or access to telecommunications data pertaining to an Australian telecommunication.

200. If this occurs, then any access to, and use of, that Australian content or metadata may be covered by the expanded immunity in proposed subsection 476.6(1). The override provision in proposed subsection 476.6(4) may be taken as an attempt to override the prohibitions in the TIA Act on accessing, and making secondary use and disclosures of, telecommunications content and data.

Recommended amendments

201. The Law Council considers that the possibility outlined above necessitates amendments to the ED Bill.

202. The ED Bill should explicitly prohibit ASD making subsequent use of, or disclosing, any Australian telecommunications content or data that it has obtained through causing a computer-related act to occur inside Australia, which invokes the expanded immunity in proposed subsection 476.6(1) of the Criminal Code.

203. Communications content or data obtained in reliance on the immunity in proposed subsection 476.6(1) should be subject to a requirement to be quarantined as soon as possible after it has been identified, and deleted as soon as possible thereafter. It should not be available to ASD, or Home Affairs, to use in the performance of their functions generally.

204. However, if there is considered to be a compelling operational case for the retention and subsequent use of such information, it should be documented in unclassified, publicly available materials, so that it can be held to scrutiny.

205. Further, if any subsequent use and disclosure is to be permitted (contrary to the Law Council's primary recommendation), this should be subject to a much higher threshold than the existing disclosure provisions in the ISA and TIA Act. That higher threshold should be in the nature of an extremely limited exception to the Law Council's recommended deletion obligation. That exception should be restricted to defined, exceptional circumstances, and a strict test of necessity (and not mere utility or assistance to ASD, or another entity with which ASD is cooperating).

Recommendation 23—limitations on use of any telecommunications content and data obtained in reliance on the immunity in proposed subsection 476.6(1)

- **Proposed section 476.6 of the Criminal Code (item 6 of Schedule 2 to the ED Bill) should be amended to prohibit ASD from making any secondary use or disclosure of telecommunications content or data that has been obtained in reliance on the immunity in proposed subsection 476.6(1) in respect of a computer-related act which occurs inside Australia, but was intended to occur outside Australia.**
- **ASD should be subject to statutory requirements to quarantine any such telecommunications content or data as soon as possible once it is identified, and securely delete it as soon as possible thereafter.**

Comment on technical capability investment

206. As a broader comment, the Law Council also considers it important that the Government's strategy for investing in technical capabilities for the national intelligence community includes a focus on proportionality and privacy.

207. That is, sustained attention and resources should be devoted to developing, acquiring and using technical capabilities (particularly for computer access and exploitation, and defensive cyber security activities) that can accurately identify the location of computers and the target data held in, or accessible from, those computers; and avoid collecting or interfering with non-target computers and non-target data.

208. Long-term, indefinite reliance should not be placed on blanket legal immunities such as that proposed in new section 476.6(1) of the Criminal Code, or laws that permit the 'incidental' overcollection of non-target data provided it is deleted and not accessed or used for investigative purposes or the performance of other functions.

209. This is an important aspect of the policy imperative for laws to keep pace with technological developments. Just as security agencies understandably seek updates to outdated laws that may restrict or prevent them from taking full advantage of new technologies in performing their functions, it is equally important that 'permissive' provisions conferring powers and immunities on those agencies are not permanently framed on the basis of present limitations in technical capabilities in precisely identifying the things being targeted.

210. It is also important that the existence of such permissible provisions do not create a disincentive to research and development to refine the precision and privacy protections in technical capabilities.

211. To this end, the Law Council recommends that the expanded immunity in proposed subsection 476.6(1) for computer-related acts done in Australia is subject to a sunset clause with a prior statutory review to determine whether it remains necessary, in line with technological developments that may better enable the accurate identification of the location of a target computer.

Recommendation 24—sunsetting and review of proposed s 476.6(1)

- **The expanded immunity for ASD in proposed subsection 476.6(1) of the Criminal Code, in relation to computer-related acts done <u>in Australia</u>, should be amended as follows:**

- **it should be subject to a five-year sunset clause, after which time it will cease to have effect unless extended legislatively; and**

- **to inform Parliamentary decision-making about possible extension, there should be a requirement for a statutory review to consider whether the immunity remains necessary, including in view of technical capabilities available to ASD to ascertain the true location of a target computer.**

  This review should be undertaken by the PJCIS (with access to appropriate independent expert technical advice); or another independent expert appointed by the Government with the agreement of the Opposition.

Proposed IGIS notification requirements

212. The Law Council welcomes the requirement in proposed subsection 476.6(8) of the Criminal Code for ASD to notify the IGIS, in writing, if it engages in conduct that enlivens the immunity, which also causes material damage to, interference with, or obstruction of, a computer in Australia.

213. This notification requirement has the potential to assist the IGIS in focusing their oversight on such activities. This includes considering whether to recommend that ASD pay compensation or make other reparations to persons who are adversely affected by a computer-related act that ASD has caused to occur in Australia; and considering whether to issue an evidentiary certificate that the actions of ASD were done in the proper performance of that agency's functions.

214. By extension, the IGIS notification requirement is also likely to require ASD to implement systems and processes to monitor the impacts of its computer-related acts, particularly to ascertain whether they have had any unforeseen impacts on the operation of computers within Australia, despite ASD's best endeavours to avoid this risk from materialising.

215. It would be open to the IGIS to form a view that the standards of propriety in relation to the use of the expanded immunity require ASD to implement such monitoring arrangements (in addition to ASD implementing systems and processes to ensure that it takes all reasonable steps to prevent this risk from arising, when planning and executing operations that involve causing a computer-related act to occur overseas).

216. Given the importance of the notification requirement to effective oversight, the Law Council is concerned that its scope is too narrow in three respects.

Acts which are likely to cause material damage, interference or obstruction

217. First, proposed subsection 476.6(8) would only require ASD to notify IGIS of computer-related acts which ASD **knows have caused** material damage to, interference with, or obstruction of, a computer.

218. There is no reporting requirement if ASD is aware that it has caused a computer-related act to occur, which is **reasonably likely to cause** material interference, loss or damage, but ASD does not categorically know whether this result has, in fact, occurred. This circumstance could arise if ASD is unable to trace the results of its actions, or if there is a delay in the onset of the reasonably foreseeable impacts of a computer-related act, whether intentional or otherwise.

219. The Law Council considers that the threshold for notifying the IGIS should be ASD's awareness of the **likely impact** of its actions. That is, if ASD is aware of a real and not remote possibility of such impacts, then it should be required to notify the IGIS and provide details of its actions and the likely impacts it has identified.

Importation of criminal fault elements as a pre-condition to IGIS notification

220. Secondly, the notification requirement in proposed subsection 476.6(8) applies only if the ASD staff member who engages in the action would '**commit an offence'** but for the immunity in proposed subsection 476.6(1) or (2) (as applicable).

221. As the Criminal Code provides that an offence consists of physical and fault elements,[34] the Law Council is concerned that the reporting obligation would technically only apply if ASD considered that its staff member had satisfied the requisite **fault elements** for a computer offence in Part 10.7 of the Criminal Code (or any other offence against an Australian law) as well as the physical elements. This could result in underreporting to IGIS, or a misunderstanding among ASD staff members of the circumstances in which such reporting must occur.

222. The Law Council considers that this potential loophole or source of confusion should be removed. Proposed subsection 476.6(8) should make explicit that the IGIS notification obligation applies if the person has engaged in conduct of the kind that is specified in subsections 476.6(1) and (2), which also satisfied the **physical elements** of a computer offence against Part 10.7 of the Criminal Code, or any other offence against a law of the Commonwealth or a State or Territory.

Acts for which ASIO would require a warrant or an authorisation to do in Australia

223. Thirdly, as noted above, the immunity in proposed subsection 476.6(1) is not subject to the exclusion in proposed subsection 476.6(3) in relation to acts for which ASIO would require a warrant or authorisation to do in Australia. (That is, the interception of telecommunications; accessing stored telecommunications or telecommunications data; or accessing or manipulating data that is held on, or is accessible from, a computer.) Rather, the exclusion of such acts in proposed subsection 476.6(3) applies only to the immunity in proposed subsection 476.6(2) for preparatory and ancillary acts.

224. Accordingly, the Law Council recommends that ASD should also be required to notify the IGIS in the following circumstances, irrespective of whether its actions cause any damage to, interference with or obstruction of, a computer:

- ***if ASD relies on the immunity in proposed subsection 476.6(1), and in doing so, it does an act or thing in Australia for which ASIO would need a warrant or an authorisation***. That is, the IGIS notification obligation should apply if ASD intends to cause a computer-related act to occur outside Australia, but this, in fact, occurs within Australia, and in the process, ASD (likely unintentionally) intercepts a telecommunication, accesses a stored communication or telecommunications data, or accesses data held on or accessible from a computer in Australia; or

- ***if ASD does preparatory or ancillary acts in Australia, but it exceeds the scope of the immunity in proposed subsection 476.6(2)***. That is, the IGIS notification obligation should apply if ASD undertakes a preparatory or ancillary activity in Australia, but in doing that preparatory or ancillary activity, contravenes the exclusion in proposed subsection 467.6(3) for intercepting telecommunications; accessing stored communications or telecommunications

[34] Criminal Code, sections 3.1 and 3.2.

data; or accessing or manipulating data held on, or accessible from, a computer in Australia.

225. This notification requirement will ensure that IGIS is alerted, in a timely manner, to legislative breaches that involve the use of intrusive collection powers in relation to Australian telecommunications content or data. This, in turn, could facilitate oversight by IGIS of ASD's remedial actions in relation to such content or data.

Recommended amendments

226. To address the issues outlined above, the Law Council recommends three amendments to proposed subsection 476.6(8) of the Criminal Code, as follows:

Recommendation 25—ASD's obligations to provide written notifications to IGIS

- **Proposed subsection 476.6(8) of the Criminal Code (item 6 of Schedule 2 to the ED Bill) should be amended as follows:**
  - **ASD should be required to notify the IGIS if it becomes aware that its conduct is reasonably likely to cause material damage to, interference with, or obstruction of a computer that is in Australia;**
  - **ASD should be required to notify the IGIS if one of its staff members engages in conduct that would satisfy the physical elements of an offence in Part 10.7 of the Criminal Code, or any other offence against a Commonwealth, State or Territory law. (That is, the notification obligation should not apply if the relevant ASD staff member or members would otherwise 'commit an offence', as this may import an assessment, by ASD, of whether the fault elements of the applicable offence were satisfied); and**
  - **ASD should be required to notify the IGIS if it engages in conduct listed in proposed subsection 476.6(1) or (2), which results in a staff member of ASD doing, in Australia, an act or thing for which ASIO would require a warrant or an authorisation to do in Australia. (That is, intercepting a telecommunication; accessing a stored communication or telecommunications data; or accessing or manipulating data held in, or accessible from, a computer).**