Law Council
OF AUSTRALIA

Office of the President

4 November 2024

Senator Raff Ciccone
Chair, Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

By email: pjcis@aph.gov.au

Dear Chair

Cyber Security Legislative Package: Responses to questions on notice

On 1 November 2024, representatives from the Law Council of Australia appeared before the Parliamentary Joint Committee on Intelligence and Security in relation to the review of the Cyber Security Legislative Package 2024.

The Law Council took two questions on notice at the hearing. Noting the short timeframe provided for responses, we have not been able to provide the level of analysis that might otherwise be expected of our answers. However, we trust that the information below will be of use to the Committee. We have also included additional comments which have subsequently been provided by the Victorian Bar in relation to the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024 (Cth) (the **SOCI Bill**).

Cyber Incident Review Board

In the course of the hearing, the Chair queried whether the Law Council held concerns about the requirement that the Minister approve the terms of reference for a review by the Cyber Incident Review Board (the **Board**) at paragraph 46(2)(c) of the Cyber Security Bill 2024 (the **Bill**).

The Law Council has previously suggested that consideration should be given to removing the requirement that the Minister approve terms of reference for a review, in order to preserve the Board's actual, and perceived, independence in the community.[1] Our concern primarily relates to the terms of reference for a review being required to identify participating standing members of the Board (section 46(4)(b)) and set parameters around the appointment of Expert Panel members (subsection 70(3)).

One way to address this concern would be to ensure that rules created under Part 5 of the Bill provide administrative guidance regarding the considerations that must be taken into account by the Minister when determining members of the Board and Expert Panellists to undertake a review. These considerations could include the independence of the appointees, and satisfaction as to the knowledge and expertise of the individuals relevant to the proposed review.

[1] Law Council of Australia, *Submission to the Cyber Security Legislation Package 2024* (31 October 2024), [61]

Telephone +61 2 6246 3788 • *Email* mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612 • Level 1, MODE3, 24 Lonsdale Street, Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

Alternatively, the nomination of standing members of the Board to participate in a review (and selection of Expert Panel members) could be a matter determined by the Chair of the Board, which is likely to avoid any perception of a fettering of independence.

Use of disclosed information in subsequent legal proceedings

During the hearing, the Deputy Chair asked the Law Council to consider whether there are likely to be circumstances where information provided either compulsorily[2] or voluntarily[3] under the Bill could be used in future legal proceedings.

While we are satisfied that there are appropriate safeguards regulating the admissibility[4] of material provided by an entity in future legal proceedings, with respect to information either reported following a ransomware payment report, or provided to the National Cyber Security Coordinator or Board,[5] we remain concerned about derivative use of that material (by a secondary Commonwealth body or prescribed State body).

In our assessment, uncertainty regarding scope for derivative use is likely to undermine the policy objectives sought to be achieved in the context of both voluntary and mandatory disclosure regimes.

We consider the most important elements of the definition of 'permitted cyber security purpose' in section 10 of the Bill to be related to responding to, mitigating or resolving a cyber security incident, preventing or mitigating material risks to social or economic stability and national security and enabling more sophisticated analysis of cyber security trends across government. Information sharing provisions should be adapted to that context.

As noted in the Explanatory Memorandum, the limited use provisions do not amount to a 'safe harbour' which shields a reporting business entity from subsequent legal liability.[6]

For instance, while reported material must not be recorded, used or disclosed for the purposes of investigating or enforcing, or assisting in the investigation or enforcement of, any contravention by the reporting business entity of a Commonwealth, State or Territory law, this will not extend to a contravention by the reporting business entity of a law that imposes a penalty or sanction for a criminal offence.[7]

As such, the limited use provisions are not intended to restrict law enforcement or regulators from gathering this information through another avenue, using their own existing powers, and using that information for regulatory or law enforcement purposes against the entity.[8]

Noting that there are a range of purposes (albeit limited) for which information can be disclosed to other bodies without the consent of the reporting body, and the possibility of subsequent criminal prosecution, the we note that there may be scope to consider a 'safe harbour' from

[2] See for example, a ransomware payment report given by an entity, Cyber Security Bill 2024 (Cth), subsection 27(1).
[3] See for example, where an impacted entity may voluntarily provide information to the National Cyber Security Coordinator about a cyber security incident that has occurred, is occurring or is imminent or a major cyber security incident that may potentially occur Cyber Security Bill 2024 (Cth), section 35.
[4] As was explained in our evidence, there is an important distinction between admissibility (as evidence in a legal proceeding based on the rules of evidence) and use. In certain contexts, the rules of evidence will not apply.
[5] See, Cyber Security Bill 2024 (Cth), sections 32, 42 and 58. Exceptions relate to criminal proceedings relating to the operation of the Bill, coronial or Royal Commission proceedings, or proceedings in which a writ of mandamus or prohibition or an injunction is sought against an officer of the Commonwealth.
[6] Explanatory Memorandum, Cyber Security Bill 2024, 7
[7] See for example, in relation to limitations on secondary use and disclosure of information in ransomware payment reports: section 30(3). See also, in relation to use and disclosure by National Cyber Security Coordinator of information voluntarily provided in relation to a significant cyber security incident, section 38(2).
[8] Explanatory Memorandum, 60 [296].

the various sanctions laws where a ransom has been paid (following reasonable due diligence on the threat actor) to encourage reporting of the ransom payment.

Additional remarks: SOCI Bill

Since lodging our primary submission, the Law Council has received additional comments from the Victorian Bar about the SOCI Bill.

Clause 3 of Schedule 1 to the SOCI Bill will amend section 9 of the *Security of Critical Infrastructure Act 2018* (Cth) (the **SOCI Act**) by extending the operation of the obligations relating to critical infrastructure assets to all data storage systems owned or operated by the responsible entity for the asset which hold 'business critical data' and which are used, or are to be used, 'in connection with' the asset. The formulation 'used in connection with' appears repeatedly in the SOCI Act but, in this context, is notably broad.

The Victorian Bar has noted that paragraph 9(1)(d) of the SOCI Act already captures data storage which itself is 'critical' and section 5 defines 'data storage' as meaning 'data storage that involves information technology and includes data back-up' ('data storage system' is undefined). Given that the proposed reform will extend to all data storage 'used ... in connection with' the critical infrastructure asset, providing 'business critical data' is stored, the definition might inadvertently capture devices, platforms and tools that do not relate to the functioning of the critical infrastructure asset.

The breadth of the potential application of the amendment is compounded by the potential extraterritorial operation of the new subsection (while section 9(2B) of the SOCI Act excludes assets located outside Australia from the definition of critical infrastructure asset, there is no equivalent proposed exclusion in relation to data storage).

The Explanatory Memorandum summarises the aim of this amendment as follows:

> *… to expand the definition of all types of critical infrastructure assets to include secondary assets which hold 'business critical data' and relate to the functioning of the primary asset.*[9]

The Victorian Bar suggests that this narrower application should be replicated in the text of the amendment by removing proposed ss 9(7)(b) and (c).

Contact

If you would like to discuss further, please contact Mr Nathan MacDonald, Deputy General Manager of Policy [redacted].

Yours sincerely

Greg McIntyre SC
President

[9] Explanatory Memorandum: Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024, 3.