THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:BMns120224

12 February 2024

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
Braddon ACT 2612

By email: shounok.chatterjee@lawcouncil.au

Dear Dr Popple,

2023-2030 Australian Cyber Security Strategy: Legislative Reforms – Consultation Paper

Thank you for the opportunity to contribute to the Law Council's submission to the Department of Home Affairs (Department) on its Consultation Paper entitled '2023-2030 Australian Cyber Security Strategy: Legislative Reforms' (Consultation Paper). The Law Society's Privacy and Data Law Committee has contributed to this submission.

Measure 2 – Ransomware reporting for businesses

Under Measure 2, the Consultation Paper proposes to establish two new reporting requirements on relevant entities, namely:

- if an entity is impacted by a ransomware or cyber extortion attack and receives a demand to make a payment to decrypt its data or prevent its data from being sold or released; or
- if an entity makes a ransomware or extortion payment.[1]

We note that the Department is seeking feedback on the nature and scope of these obligations, including which entities should be subject to the proposed requirements, the types of mandatory information required to be reported, and the timeframe for reporting.

Types of entities

In seeking to minimise the potential regulatory burden caused by additional ransomware reporting obligations, the Consultation Paper notes:

> …it may be appropriate to acquit the proposed ransomware reporting obligation through existing reporting obligations. In some cases, an entity may be subject to other incident reporting obligations that could collect the relevant information about a ransomware or cyber extortion incident. For example, approximately 1,000 Australian entities fall under the mandatory cyber incident reporting obligations under the SOCI Act…[2]

[1] Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy: Legislative Reforms*, (Consultation Paper, December 2023), 14.
[2] Ibid, 15.

We suggest that, in addition to considering consolidating the proposed new obligations with existing reporting obligations under the *Security of Critical Infrastructure Act 2018* (SOCI Act), consideration should also be given to consolidating, where possible, the proposed ransomware reporting obligations with existing reporting obligations under the Notifiable Data Breaches (NDB) Scheme and the *Privacy Act 1988* (Privacy Act). In our view, the NDB Scheme and Privacy Act should inform both the types of entities captured by the new requirements, and the timeframes for reporting, in order to promote consistency in the relevant law and minimise regulatory burden.

Consideration of which entities should be subject to the proposed requirements under Measure 2 is somewhat complicated by the ongoing review of the Privacy Act. While the Government has 'agreed in-principle' to removing the small business exemption from the Privacy Act, we note that this is subject to "further consultation… with small businesses and their representatives on the impact that removing the small business exemption would have."[3]

In our view, an effective ransomware reporting regime that is developed to "accelerate law enforcement action, enhance whole-of-economy risk mitigation and help tailor victim support services"[4] should be broadly applicable across the economy, and should not be limited to large entities only.

If the small business exemption is removed from the Privacy Act, we suggest that the proposed ransomware reporting requirements for small businesses should be consistent with their other reporting requirements under the NDB Scheme and Privacy Act. However, subject to the outcome of the Government's further consultations with small businesses, consideration could also be given to introducing a more streamlined mandatory reporting process for small businesses, to reduce the regulatory burden of Measure 2.

We note the Department is also seeking views on the extent to which the proposed 'no fault' and 'no liability' principles would encourage entities to report ransomware attacks. While we see merit in adopting a no fault and no liability approach, we suggest that further clarification is required regarding how, in practice, these principles would interact with entities' existing legislative and regulatory obligations in dealing with a relevant cyber incident. For example, it is not clear how information reported under Measure 2 would be treated under the Commonwealth freedom of information regime, which we note is also currently under review by Government.[5] It will be important to explicitly address the evidentiary status of any notifications, reports and related communications in any litigation, prosecutions or investigations that may be triggered by a given incident.

<u>Types of information</u>

The Consultation Paper sets out various types of information that could fall within the Measure 2 reporting requirements, including:

- when the incident occurred, and when the entity became aware of the incident;
- what variant of ransomware was used (if relevant);
- what vulnerabilities in the entity's system were exploited by the attack (if known);
- what assets and data were affected by the incident;
- what quantum of payment has been demanded by the ransomware actor or cybercriminal, and what method of payment has been demanded;

[3] Australian Government, *Government Response: Privacy Act Review Report*, (September 2023), 6.
[4] Above n 1, 13.
[5] Legal and Constitutional Affairs References Committee, *The operation of Commonwealth Freedom of Information (FOI) laws*, Report (December 2023).

- the nature and timing of any communications between the entity and the ransomware actor or cybercriminal;
- the impact of the incident, including impacts on the entity's infrastructure and customers; and
- any other relevant information about the incident or actor that could assist law enforcement and intelligence agencies with mitigating the impact of the incident and preventing future incidents.[6]

While we see merit in having this information form part of the relevant reports, we note that certain information, such as "what assets and data were affected" and "the impact of the incident", can be highly complex and may take significant time to fully ascertain. In some cases, it simply may not be possible to provide this information comprehensively within a short period, particularly if the timeframe for reporting is to align with, for example, the 72-hour timeframe to report cyber incidents under the SOCI Act.

We also note that, in the experience of our members, the targets of ransomware attacks often do not have in place adequate processes to engage a cyber incident investigation team, which contributes to further delays in handling and responding to ransomware attacks. Similar delays would also naturally be incurred under the proposed ransomware reporting regime.

Accordingly, we suggest that any proposals under Measure 2 should account for the practical difficulty in providing a complete snapshot of ransomware attacks in a limited timeframe and should allow for further information to be subsequently furnished by victims of ransomware attacks as it becomes known.

In addition, we note there may be further complications where legal advice forms part of the incident response to a ransomware attack. The proposed reporting structures will need to address the professional obligations of confidentiality that attach to communications in those circumstances.

Measure 3 – Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

<u>Uses and sharing of information</u>

Measure 3 effectively proposes to establish a legislated 'limited use' obligation for the Australian Signals Directorate (ASD) and the National Cyber Security Coordinator (Cyber Coordinator) in respect of cyber incident information they receive. This is to encourage industry engagement with government following a cyber incident.

Under the limited use obligation, information shared with ASD or the Cyber Coordinator would be limited to 'prescribed cyber security purposes' defined in legislation, and could not be used by regulatory agencies for investigative or compliance action. The Consultation Paper provides a range of possible uses that may constitute prescribed cyber security purposes.[7]

However, we note that the Consultation Paper seeks to clearly delineate between the limited 'use' of relevant information and the 'sharing' of such information. It notes:

> It is important that any limited use obligation does not preclude ASD and the Cyber Coordinator from sharing appropriate information with other agencies – including law enforcement, national security, intelligence agencies and regulators. The proposed

[6] Above n 1, 15.
[7] Ibid, 20.

> model of a 'limited use' obligation would restrict the use of cyber incident information, but not the sharing of this information.[8]

In our view, significant further clarification is required in relation to the ASD's and Cyber Coordinator's information sharing powers, particularly with regard to:

- The types of information that can be shared with other agencies. In this regard, we note that certain types of information, such as assets and data affected by ransomware or personal information relating to customers, are more sensitive than other forms of information, such as the type of ransomware used in the attack.
- The purpose(s) for which relevant information can be shared, and what, if any, restrictions on the information sharing powers are proposed, for example, on derivative use by those agencies with whom the information is shared.

Information sharing with industry

The Consultation Paper proposes that a prescribed cyber security purpose under Measure 3 is "to analyse and report trends across the cyber threat landscape, including the provision of anonymised cyber threat intelligence to government, industry and international cyber partners."[9] In our view, cyber security providers play a key role in driving widespread cyber security uplift across the economy. Accordingly, we support, in principle, the use of cyber threat information to report trends in the cyber threat landscape to industry, provided the information is appropriately anonymised.

We also suggest that in addition to the Measure 3 proposals, which seek to promote and incentivise the sharing of cyber incident information with government, consideration should be given to instituting similar 'limited use' provisions to enable cyber security organisations (including managed service providers) to use, for the purpose of analysis, and share information about a cyber incident affecting one or more of their customers, without a breach of contract or confidence. As noted above, in the case of law firms, express consideration will need to be given to the professional duties of legal advisers and their role in various information sharing arrangements, and pending investigations, if any.

In the experience of our members, it is common for private and public sector consumers of cyber security services to seek to prevent any discussion or information sharing relating to cyber incidents, particularly given the significant reputational risks involved. Cyber security contracts often contain very strict confidentiality requirements, and prohibitions on disclosing any information on counterparties (including their security providers).

A limited use provision enabling cyber security organisations to share information, in limited circumstances, may assist in enabling a more efficient and coordinated response to cyber incidents. Of course, this would involve a range of additional considerations, which may require further consideration and discussion.

Measure 4 – Learning lessons after cyber incidents – A Cyber Incident Review Board

General comments

We note that the essential purpose of the proposed Cyber Incident Review Board (CIRB) is to conduct no fault, post-incident reviews of cyber incidents and to promote collective cyber security by publicly sharing findings and best practice guidance. The Consultation Paper notes that the CIRB is not a law enforcement, intelligence or regulatory body, and its proposed functions should not:

[8] Ibid, 21.
[9] Ibid, 20.

- Prejudice or interfere with ongoing activities of law enforcement, national security and intelligence agencies, regulators and judicial bodies; nor
- Have any regulatory function itself.[10]

As a broad observation, we note that this would require a high level of coordination between the CIRB and a large number of federal and state agencies operating within the law enforcement, national security, privacy and data law spheres, and may pose considerable practical difficulties. There is also a risk that carving out certain information, so as not to prejudice or interfere with ongoing legal or regulatory activities, may result in an incomplete picture of the relevant cyber incident, or lead to significant delays in the CIRB carrying out an incident review. In our view, the utility of the CIRB's incident reviews is largely contingent on its ability to perform its functions in a timely and accurate manner.

We also consider that the proposed CIRB is, itself, likely to become a high priority target for cyber threat actors, particularly given its proposed investigatory powers. Accordingly, we suggest that the CIRB should be equipped with industry leading information security controls and standards (and ensure each of its members meet these standards) and should be appropriately resourced to ensure it maintains highly robust cyber security measures.

Sensitive information

While the CIRB's role includes making public recommendations, the Consultation Paper contemplates including a mechanism to ensure that certain sensitive information relating to cyber incidents remains appropriately confidential. For example, the Consultation Paper notes:

> Potential safeguards to protect sensitive information could include granting the CIRB powers to provide confidential reports to Government and producing redacted reports for public consideration.[11]

In this regard, we suggest that some guidance may be gleaned from existing legislation relating to independent reviews. For example, Part 2A, Division 4 of the *Health Administration Act 1982* (NSW), which relates to root cause analysis in the NSW public health system, sets restrictions on the types of incidents that can be reviewed[12] and what information can be disclosed by an incident reviewer;[13] and prohibits information being given in evidence or advice, or reports from the review being admitted in evidence.[14]

We hope this input is of assistance. Please contact Nathan Saad, Policy Lawyer, on (02) 9926 0174 or nathan.saad@lawsociety.com.au in the first instance if you have any queries.

Yours sincerely,

Brett McGrath
President

[10] Ibid, 24.
[11] Ibid, 28.
[12] *Health Administration Act 1982* (NSW) s 21M.
[13] Ibid, s 21N.
[14] Ibid, ss 21O and 21P.