1 March 2024

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

By email to: AusCyberStrategy@homeaffairs.gov.au

ASX SUBMISSION – CYBER SECURITY LEGISLATIVE REFORMS: CONSULTATION ON PROPOSED NEW CYBER SECURITY LEGISLATION AND ON CHANGES TO THE *SECURITY OF CRITICAL INFRASTRUCTURE ACT* 2018

ASX welcomes the opportunity to provide a submission on the proposed new cyber security legislation and changes to the *Security of Critical Infrastructure Act 2018* (**SOCI Act**). Recent major cyber incidents in Australia have highlighted the importance of cyber resilience for all entities. ASX recognises and welcomes the Government's intention and commitment to bolstering Australia's cyber security, and in particular, the Government's approach of situating these reforms within a broader, whole-of-government strategy.

As the Government's 2023–2030 Australian Cyber Security Strategy makes clear, responsibility for cyber security is shared across the community. Corporate Australia, and in particular, the operators of critical infrastructure, play a key role in shaping Australia's cyber resilience.

As a key provider of critical market infrastructure and clearing and settlement facilities in Australia, ASX recognises cyber risk as one of the most critical risks to be managed and mitigated. ASX has a cyber security strategy in place and continually looks to improve capability, and leverage better practices and relevant international standards. The strategy is developed through an assessment of a number of information sources, including the risks to ASX's operating environment, the current and future threat environment, industry research and benchmarking, results of audits and penetration tests and an analysis of incidents and key risk indicators.

Background

Parts of the ASX Group are subject to the SOCI Act as the responsible entities for critical infrastructure assets in the financial services and markets sector. At present, the obligation to adopt, maintain and comply with a written risk management program has not been applied to critical infrastructure assets within the financial markets sector on the basis of existing regulatory oversight by the relevant regulatory agencies.

ASX is both a market operator, and listed on the ASX market. Listed entities must comply with ASX Listing Rule 3.1, which provides that once an entity is or becomes aware of any information concerning it that a reasonable person would expect to have a material effect on the price or value of the entity's securities, the entity must immediately tell ASX that information. This immediate disclosure obligation is subject to some limited carve outs in ASX Listing Rule 3.1A that are premised on the information remaining confidential (in addition to other requirements). In the event of a cyber incident, a listed entity's Board and management will need to have regard to the entity's ongoing continuous disclosure obligations.

ASX has provided comment on a number of the proposals in the Consultation Paper, from the position of both a market operator and entity subject to obligations under the SOCI Act. ASX notes that ultimately, assessment of the legislative reforms will be contingent on the final drafting of the relevant legislative provisions and as such, ASX encourages a consultation process that allows adequate consideration of the draft legislation by impacted stakeholders.

Mandatory no-fault, no-liability reporting obligation for ransomware attacks

ASX recognises the value of improved visibility of ransomware incidents and supports in principle the proposal to establish a no-fault and no-liability ransomware reporting obligation.

ASX considers there is merit in the proposed ransomware reporting obligation being consolidated with the existing mandatory cyber incident reporting obligation under the SOCI Act. This will minimise regulatory duplication and ensure

clarity around the obligations that apply in the wake of a cyber incident. This is also likely to lead to more consistent compliance and therefore greater visibility of the cyber threat picture.

With regard to the information to be reported under the proposed obligation and the timeliness of such reporting, ASX encourages that an appropriate balance is struck between providing access to useful information about the ransomware threat environment and minimising the regulatory burden on entities that are dealing with the consequences of a cyber incident.

ASX supports public reporting of anonymised and aggregated information collected under the ransomware reporting obligation. This information should provide a comprehensive overview of the cyber threat environment and an outline of the types of threats that are likely to emerge or recede in future. The information presented should contain a level of detail sufficient to support entities in responding to emerging cyber threats.

In formulating the legislation to implement the new reporting requirement, it will be critical to ensure that the no-fault, no-liability principles do not operate to absolve businesses of responsibility for their cyber security arrangements. Entities should remain accountable for their risk management arrangements, including under the SOCI Act, while reporting significant incidents.

Limited use obligation

ASX supports the proposal for a limited use obligation regarding how cyber incident information shared with the Australian Signals Directorate (**ASD**) and the Cyber Coordinator is used. Clarifying the uses of information provided by entities will support confidence in the SOCI Act regulatory regime and remove disincentives for entities subject to a cyber incident to engage with ASD and the Department of Home Affairs.

The Consultation Paper proposes a list of proposed 'prescribed cyber security purposes' for the sharing and use of incident information received and collected by ASD. ASX submits that the legislative provisions setting out 'prescribed cyber security purposes' should be prescriptive and exhaustive to give confidence to industry about how the collected information can and will be used. These prescribed purposes should be limited to facilitating the prevention, mitigation, and management of cyber incidents, and for informing intelligence and national security agencies about the cyber risk environment.

ASX does not support allowing the information collected by ASD and the Cyber Coordinator to be used in any regulatory or enforcement proceeding, as this would undermine the core objective of removing a disincentive to disclosure. ASX suggests consideration be given to an express prohibition on the uses of information for such purposes, including by other regulatory agencies where such information has been shared for the purpose of responding to an incident.

Any information that is shared with government departments or agencies consistent with the 'limited use' framework should be shared only on a confidential basis, with legal obligations imposed on those agencies to maintain the confidentiality of the information. If information that a listed entity reports under the proposed ransomware reporting obligation ceases to be confidential, that would deny the listed entity the ability to rely on the carve outs from immediate disclosure in Listing Rule 3.1A even if the other requirements of that rule are met in relation to the information. This could result in premature disclosure to the market of materially price sensitive information that would otherwise be insufficiently definite to warrant disclosure. This could put listed entities in a more difficult position than other entities subject to the proposed ransomware reporting obligation.

Cyber Incident Review Board

The proposed Cyber Incident Review Board (**CIRB**) will, by its nature, collect a significant amount of sensitive information about entities' cyber incidents. The legislation establishing the CIRB should reflect this, and include design features to ensure that the CIRB can protect sensitive information, including in any interactions with other disclosure obligations (for example, the *Freedom of Information Act 1982*).

ASX supports the introduction of a limited use obligation with respect to any information gathered by the CIRB. Such an obligation would support engagement with the CIRB and ensure that reviews of the CIRB are no-fault and no-blame. It will be important to ensure that entities can be confident that they will not expose themselves to legal liability for compliance with the CIRB's information gathering powers.

Data storage systems and business critical data

ASX acknowledges the risks to data storage systems and business critical data and accepts that certain business critical data may warrant protection under the SOCI Act if it could be used to assist an attack against a critical infrastructure asset. ASX supports extending SOCI Act requirements to such data and the systems holding it.

ASX is supportive of limiting regulatory duplication and implementing these reforms in close consultation with other agencies and regulators to ensure security outcomes are achieved with minimal regulatory burden. This is particularly important for the financial services and markets sector which is subject to close oversight by financial regulators.

Ministerial power to manage secondary consequences of a cyber-incident

ASX supports in principle the proposed last resort directions power for the Minister for managing the secondary consequences of a cyber incident. However, given the broad range of directions that are contemplated under the proposed power, the enabling legislation should make clear that this power is only to be used as a last resort.

ASX also submits that in formulating the draft legislation giving effect to the proposed directions power, the Government should provide for safeguards and controls on its exercise, such as substantive and procedural conditions governing its use. The consultation paper outlines a number of such safeguards and controls. In particular ASX supports:

- legislated purposes for which a direction may be given;
- consultation requirements with the affected entity and relevant state and federal Ministers, departments and regulatory bodies, particularly where there are interactions with the *Privacy Act 1988*; and
- immunities for acts done in compliance with a direction.

ASX supports the position outlined in the consultation paper that the directions power would not be used in a manner that conflicts with other regulatory frameworks, and that the Government would coordinate its actions between regulatory agencies. This is particularly salient for ASX, which is subject to oversight functions which may overlap, or could give rise to a potential conflict with, the powers of regulators under the SOCI Act. For example, ASIC has a number of directions powers with respect to ASX which could be used during a cyber incident.

ASX also notes Treasury's proposed legislation providing for crisis management powers in respect of financial market infrastructures. While the legislation is currently being finalised in advance of introduction to Parliament, the exposure draft legislation provides for a number of powers exercisable for the management of a crisis in financial market infrastructures. It is possible that the proposed directions power may overlap with these powers in the event of a serious cyber incident affecting Australian financial market infrastructure. As such, it will be important to ensure that there are appropriate mechanisms to ensure coordination between ASX's regulators and the Department and Minister of Home Affairs in the event of an incident which might require that this direction – or any other SOCI powers – be deployed. This will prevent confusion and regulatory duplication during a period when an entity facing a cyber incident will need to focus on resolving the incident and any secondary effects.

ASX would welcome the opportunity to discuss the matters raised in this submission in more detail. If you have any questions, please contact me on the details below.

Yours sincerely

Diane Lewis
GM, Regulatory Strategy and Executive Advisor
[redacted]