2023-2030 Australian Cyber Security Strategy: Legislative Reforms

SUBMISSION - March 2024

Ai Group Submission to the 2023-2030 Australian Cyber Security Legislative Reforms Consultation Paper

Ai Group welcomes the opportunity to respond to the 2023-2030 Australian Cyber Security Strategy Legislative Reforms Consultation Paper. This submission relates to proposed new cyber security legislation.

Ai Group agrees there is a need for new cyber security legislation to be developed to support the objectives of the National Cyber Security Strategy.

Increases in the frequency, severity and sophistication of cybersecurity incidents warrant the development of more contemporary regulatory frameworks. The increasing digitalisation of the economy – across both consumer and industrial sectors – will bring transformative opportunities for Australia while also posing greater cyber exposure. Keeping cyber regulation up to date with this evolving landscape is critical for national economic security.

However, all regulation inherently involves striking a balance between security and efficiency. While under-regulation leaves Australia exposed to cyber risk, over-regulation may stifle innovation and new opportunities in the economy.

Regulatory measures adopted as part of this legislative agenda should consider the balance between cyber security and business innovation and digitisation. It is imperative that regulation be supportive of the efforts by industry to enhance its cyber capabilities. Regulation should be designed in a way that is practical for widespread uptake amongst industry, imposes least-cost compliance burden, and supports rather than inhibits confidence in broader digital upgrading by industry.

Businesses facing cyber-attacks are victims of a crime and should be treated as such. Punitive measures should be directed at the perpetrators of crimes, not the victims.

Collaborative frameworks should be focus of holistic uplift in cyber capability

Ai Group argues that Government should complement legislative instruments with other consultative policy measures that guide, support, and collaborate with businesses to improve enterprise capability.

Government should give proper consideration to non-regulatory options to address inhibitors that reduce the incentive for business to invest in digitalisation and cyber

security. Where legislation is used, language should be clear, direct and practical for implementation by industry.

As Australia's cyber regulations are created or amended, complementary efforts to support cyber capability uplift in Australian industry must be undertaken. National cyber security is a function of both *regulation* (which determines the behaviours businesses must undertake) and *industry capability* (which determines their ability to meet these behaviours).

An increase in regulation without a corresponding increase in business capability will not genuinely improve Australia's cyber resilience and achieve the aims of the *2023-2030 Australian Cyber Security Strategy*.

Secure-by-design standards for Internet of Things devices

Ai Group recognises the need for Internet of Things devices to be secure in consumer settings.

While the voluntary Code of Practice: Securing the Internet of Things for Consumers aligns to the international ETSI EN 303 645 standard, businesses should have the flexibility to choose one of several specific standards to adopt.

Ai Group recommends:

- Any cyber security standard developed or used in Australia should align with international standards to minimise regulatory burden, limit the cost of compliance on industry and ensures Australia does not become isolated.

- Government should consult and collaborate with industry if they were to draw on international standards mapping, such as the C2 Consensus on IoT Device Security Baseline Capabilities.

Ransomware reporting

At the time that a business is the victim of a ransomware demand, reporting requirements need to be clear, helpful, and not adverse to their incident response and recovery efforts.

The Government is proposing to establish **two** ransomware reporting obligations.

1. 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
2. if an entity makes a ransomware or extortion payment.

The purpose of mandatory ransomware reporting is to gather information that assists with managing future attacks. The scope of ransomware reporting should be

determined principally based on the consideration of systemic risk management, and aim to compliance capability and costs for reporting entities.

Ransomware information collection should not be designed, nor should be used, to make public the experience of individual businesses who are victims of a crime.

Businesses need time to assess many factors during a cyber incident, such as if they are being extorted, the size and nature of the impact on the business, and whether a ransom request is genuine. Therefore, regulation needs to consider the purpose of the information collection and craft regulation accordingly. It must take into consideration the existing total regulatory burden businesses already face and minimise additional requirements.

It must also take into consideration the complexity of existing cyber reporting obligations. The scope of the information collected needs to be demonstrably useful to the needs of harm minimisation on the Australian economy and critical infrastructure

Ai Group does not support civil penalties for a lack of industry compliance with ransomware reporting obligations. Government needs to work collaboratively and supportively with industry for data collection needs. Victims of a ransomware attack who are being extorted are victims of a crime and should be supported during cyber-attacks.

Ai Group recommends:

- Businesses that fall under the SOCI Act should not face any additional reporting obligations, as they already have mandatory cyber incident reporting obligations under that framework (including an obligation to report ransomware within 72 hours)

- Small businesses should not be obligated to report as they have limited compliance capabilities, and do not pose significant systemic cyber risks. We propose a threshold of $10 million p.a. turnover, consistent with the definition of small business used in other policy regimes.

- Information shared under the reporting obligation will be sensitive and must be anonymised and aggregated. Not all incident reporting will be able to be anonymised or disguised in aggregate, and in such cases it should be excluded from publication.

- Anonymised summaries of the types of incidents, levels of impact and quantum of ransom payments (if any) must be of demonstrable use to minimise further cyber attacks that include ransom demands.
  Reporting obligations should be reasonable, within 14 days of a request for a ransom payment.

- Penalties should not be directed at businesses that have not met reporting obligation., Government should incentivise reporting by offering support and assistance when requested by those who report ransom requests and/or payments.

Limited use obligation for information provided to the Australian Signals Directorate (ASD) and the National Cyber Security Coordinator (Cyber Coordinator)

Ai Group welcomes and supports the limited use obligation for information provided to the Australian Signals Directorate and the National Cyber Security Coordinator.

During a cyber incident, an explicit obligation of confidentiality upon the ASD and the Cyber Coordinator is essential. Businesses need to be confident that their engagement with these entities while they are victims of a cyber threat, will not lead to any additional and unnecessary reputational damage.

Government needs to ensure a level of trust in the organisations designed to work with business. Language and practice around cyber incidents should be collaborative, supportive and designed to augment the capabilities of organisations under attack, or at risk of attacks.

Establishing a Cyber Incident Review Board

Ai Group welcomes and supports the establishment of a Cyber Incident Review Board (CIRB).

Major cyber incidents have the potential to generate lessons that can be shared publicly to prevent future attacks.

The CIRB needs to balance the outcomes of a review with the intrusions into a business and cannot be disruptive to the process of business recovery.

The scope of a CIRB must be clearly focused on ‘no fault’ reviews of significant cyber incidents of systemic impacts on national cyber security.

Consideration should be given to the reputational damage an organisation may face, and the findings of the CIRB should be focused on preventing, mitigating, and responding to future incidents in a constructive manner that benefits all parties.

CIRB findings would contribute to resources available to industry to enable cybersecurity improvements. Businesses need to be informed of developing risks and require practical and easy to use information to be able to target their cybersecurity resources effectively. The CIRB can aid in this process by providing useful information for entities to further assess evolving risks and assist businesses in focusing their resources with respect to their own distinctive cyber needs.

Ai Group recommends:

- The CIRB should operate as a 'no-fault' incident review board, conducting no-fault incident reviews to understand major cyber incidents, and publish lessons learned in reports that are usable for industry and the broader public.

- Publicly released reports should not have any information sensitive to the business or individuals and must consider reputational risk to organisations. The focus of the board should be preventative measures across all cyber users.

- Public reports or recommendations released by the CIRB should not prejudice or interfere with ongoing activities of law enforcement, national security and intelligence agencies, regulators, insurance agencies and judicial bodies.

- The CIRB criteria must be guided by public interest to manage sensitive information considered in the scope of a post-incident review, including not publicly revealing vulnerabilities, personal information or non-personal information that may expose individuals and businesses to harm.

- The CIRB should be comprised of standing members as a multi-stakeholder advisory committee. Standing members should be drawn from across the public and private sectors including industry representation. Members should be selected to combine their collective expertise. A composition of standing CIRB members would facilitate consistency in decision-making and enable CIRB members to deepen experience over the course of various CIRB reviews.

- The chair for the board should be a new, independent official able to take into consideration all stakeholders of cyber use, appointed by the Government.

- The power to initiate a CIRB review should sit with the National Cyber Security Coordinator.

- The CIRB should have limited information gathering powers to acquire information required to facilitate the review of a cyber incident.

About the Australian Industry Group

The Australian Industry Group (Ai Group®) is a peak employer organisation representing traditional, innovative and emerging industry sectors. We are a truly national organisation which has been supporting businesses across Australia for 150 years.

Ai Group is genuinely representative of Australian industry. Together with partner organisations we represent the interests of more than 60,000 businesses employing more than 1 million staff. Our members are small and large businesses in sectors including manufacturing, construction, engineering, transport & logistics, labour hire, mining services, the defence industry, civil airlines and ICT.

Our vision is for a thriving industry and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

With more than 250 staff and networks of relationships that extend beyond borders (domestic and international) we have the resources and the expertise to meet the changing needs of our membership. We provide the practical information, advice and assistance you need to run your business. Our deep experience of industrial relations and workplace law positions Ai Group as Australia's leading industrial advocate.

We listen and we support our members in facing their challenges by remaining at the cutting edge of policy debate and legislative change. We provide solution-driven advice to address business opportunities and risks.

Australian Industry Group contacts for this submission

Louise McGrath – Head of Industry Development and Policy
[redacted]

Colleen Dowling – Senior Research Analyst
[redacted]

www.aigroup.com.au