14 April 2023

Department of Home Affairs
2023-2030 Australian Cyber Security Strategy Expert Advisory Board

Email: auscyberstrategy@homeaffairs.gov.au

Dear Sir/Madam

Response to Discussion Paper: 2023-2030 Australian Cyber Security Strategy

The Actuaries Institute ('the Institute') welcomes the opportunity to comment on the Government's 2023-2030 Australian Cyber Security Strategy Discussion Paper. The Institute is the peak professional body for actuaries in Australia. Our members work in a wide range of fields including insurance, superannuation and retirement incomes, enterprise risk management, data analytics, climate change impacts and government services.

We have a longstanding commitment to contribute to public policy debates where our members have relevant expertise, including advice and policy recommendations in the Institute's 2022 Green Paper Cyber Risk and the Role of Insurance.

General comments on the Government's proposed 2023-2030 Australian Cyber Security Strategy

The Institute welcomes the intention of the 2023-2030 Australian Cyber Security Strategy given the prevalence of digital technologies and the importance of protecting Australians and the Australian economy.

Specific feedback on Cyber Security Strategy Discussions Paper Questions

We have focused our feedback on the following questions from Attachment A of the Discussion Paper.

2.a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?

The Actuaries Institute's general position is that additional cyber regulation is unlikely to be helpful. There is a high level of existing regulation around management of business risk, together with the potential for substantial fines in the case of data breaches. The pace of technological change is such that specific regulations risk being outdated before they can be implemented. There are challenges in making sure that the requirements are proportional to the size of an organisation and the specific nature of the risks.

We believe that market-driven mechanisms, accompanied by increased government cyber maturity, offer the opportunity for a more responsive and proportionate approach, especially for small and medium sized enterprises (SMEs).

Institute of Actuaries of Australia
ABN 69 000 423 656
Level 2, 50 Carrington Street, Sydney NSW 2000, Australia
t +61 (0) 2 9239 6100 **f** +61 (0) 2 9239 6170
actuaries@actuaries.asn.au | www.actuaries.asn.au

2.b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

We support a modernisation of the definition of 'critical assets' for the Act.

2.c. Should the obligations of company directors specifically address cyber security risks and consequences?

The Actuaries Institute's general position is that excessive or unnecessary regulation has the potential to obstruct the efficiency of markets, and while self-regulation should be used as a first resort, in some cases where the problem is large enough, regulatory solutions can be appropriate where proportional.

While we acknowledge that cyber security risk is a 'wicked' problem, we believe that on balance, the obligations of company directors need not specifically address cyber security risks and consequences, as:

- Risk identification and management are already core responsibilities of directors (https://asic.gov.au/regulatory-resources/corporate-governance/risk-oversight/).
- Given the growth of high-profile serious cyber incidents, we think the general level of awareness regarding cyber security as a critical source of risk facing companies is now sufficiently high that it should be front of mind for directors.
- There are existing processes and guidance in place to support company directors to identify and manage risk, including cyber risk specifically, so additional requirements would add unnecessary regulatory burden. As we note in our response to question 2.e., these obligations are already significant for cyber security.

2.e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

Cyber security regulations and legal obligations impose a significant cost to Australian businesses. Publicly available statistics on the cost of regulation are limited in Australia. However, in the US, Forbes reference that companies spend up to 40% of their cyber security budget submitting regulatory compliance reports[1]. The price of non-compliance would be even greater with companies in breach of the laws subject to fines and penalties.

To monitor the regulatory burden of cyber security laws on businesses, the Australian Government or relevant agency would need to measure the cost of regulation on business over time. Regulatory costs might include roles, staff and Board time spent on compliance, as

[1] https://www.forbes.com/sites/forbestechcouncil/2022/01/13/cutting-the-cost-and-complexity-of-cybersecurity-compliance/

well as tools and systems implemented to ensure compliance. This information could be collected through survey or consultation with a range of businesses (by size and industry).

Australian businesses are required to navigate numerous cyber security laws, regulations and frameworks to determine what rules apply and when. There is a patchwork of policies, laws and frameworks such as t*he Privacy Act*, *the Crimes Act 1914*, *the Security of Critical Infrastructure (SOCI) Act 2018*, *the Telecommunications (Interception and Access) Act 1979* and *Cyber Operational Resilience Intelligence-led Exercises (CORIE)*. There are other laws at a State and Federal level that touch on cyber security, including within *the Criminal Code Act 1995*, *the Telecommunications Sector Security Reforms (TSSR)* and the recently amended *Security of Critical Infrastructure (SOCI) Act 2018*. In our view, a single piece of legislation which aggregates the laws and requirements for business would create efficiencies and simplify the already complex world of cyber security. This single source of legislative requirement could reference other laws and regulations but would function as the starting reference point.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Cyber resilience is the ability to limit the impact of security incidents by implementing effective tools and processes[2]. Cyber security is vital in an interconnected world. However, globally there is a shortage of skilled cyber security professionals.

Given that many businesses operate across country borders, the need for harmonisation of cyber security legislation, rules and regulation is important. Alignment on cyber security standards across nations would increase the simplification and strength of cyber security globally. Consistency also means that countries can leverage training material across borders to support business and industry.

9. Would expanding the existing regime for notification of cyber security incidents (e.g., to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

We do not support further mandatory reporting to regulators unless there are specific instances or gaps which are identified. Differences in requirements between jurisdictions and stakeholders have the potential to further add to the burden during incident response. This is particularly acute for smaller organisations and those working across borders.

Public understanding is likely to be better developed by ongoing education and enhancement of government cyber security maturity.

There is value in a confidential clearinghouse for timely communication of a wider range of cyber events, such as those impacting the business continuity in a manner which is better aligned with the pressures of an incident response. This would provide an opportunity to

[2] https://www.balbix.com/blog/resilience/

identify and communicate in a timely way trends such as common threat actors or vulnerabilities.

7. What can government do to improve information sharing with industry on cyber threats?

Government should focus on making the sharing of existing information more dynamic. More dynamic sharing with industry, academia and the public can help to demonstrate the value of the information gathered and build the case for any subsequent increase in reporting requirements.

Government should also engage with industry around specific emerging issues such as the Lloyd's of London requirements around attribution for cyber war. One of the major challenges facing the cyber insurance industry is around how to address and limit systemic and accumulation risk, particularly around cyber war coverage. Insurers are grappling with how best to exclude exposure that goes beyond insurability to ensure a sustainable cyber insurance market. We believe a collaborative approach is required between government and the private sector to understand how to best address systemic threats in cyber insurance policies to help ensure companies can receive the appropriate level of cover to protect their cyber exposures.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Government should support the explicit inclusion of digital and cyber risks within a broad range of existing education programmes. This has the advantage of leveraging Australia's existing educational capabilities and helping to build a broad base of capability and awareness, beyond technology specialists.

We note that cyber threats have been growing despite record spends by government and the private sector. One of the key issues to mitigating these threats is the severe shortage of qualified cyber experts. We believe a collaborative approach is required between government and the private sector to understand and address these threats, including greater government funding for addressing the shortage of cyber specialists, joint training initiatives, and education on best practice management of risks. Whilst many cyber security courses are offered through universities and other training providers, the quality of curriculum and standard varies widely and therefore requires oversight and governance.

15.a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

We believe SMEs would benefit from the government actively playing a role to bridge the gap between awareness of the cyber threat landscape and how to adequately address this through risk mitigation solutions, including cyber insurance. Many SMEs have a limited knowledge of cyber insurance or what to do if they are attacked. This mismatch is exacerbated by a clear hardening of the cyber insurance market which has made obtaining a cyber insurance policy increasingly difficult, complex and costly. Cyber insurance take-up rate for SMEs remains low (estimated to be less than 20% in Australia by the Insurance Council

of Australia); many SMEs still consider themselves not attractive targets for hackers and that any potential consequences of a security breach would be minor. For those SMEs who wish to procure insurance, many do not have the minimum security standards that insurers require.

To support this, SMEs require cyber solutions to be more visible, policies more easily understood and products easier to assess, with government, insurers and other appropriate stakeholders all having a role to play. Part of this would require assisting SMEs in understanding and implementing the necessary security standards to purchase affordable insurance solutions. Government investment in training and education is crucial to achieve this objective.

We would be pleased to discuss this submission or to provide further information. If you would like to do so, please contact Elayne Grace, Chief Executive Officer of the Actuaries Institute, on [redacted] or [redacted].

Yours sincerely

(Signed) Naomi Edwards

President