Governance Institute of Australia

T +61 2 9223 5744 **F** +61 2 9232 7174
E info@governanceinstitute.com.au
Level 10, 5 Hunter Street, Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

27 August 2021

Cyber, Digital and Technology Policy Division
Department of Home Affairs
6 Chan St, Belconnen ACT 2617
By email: techpolicy@homeaffairs.gov.au

Dear Sir / Madam,

Strengthening Australia's cyber security regulations and incentives

Who we are

Governance Institute of Australia is a national membership association, advocating for our network of 40,000 governance and risk management professionals from the listed, unlisted, public, not-for-profit and charity sectors.

As the only Australian provider of chartered governance accreditation, we offer a range of short courses, certificates and postgraduate study. Our mission is to drive better governance in all organisations, which will in turn create a stronger, better society.

Our members have primary responsibility for developing and implementing governance frameworks in public listed, unlisted and private companies, as well as not-for-profit organisations and the public sector. They have a thorough working knowledge of the operations of the markets and the needs of investors. We regularly contribute to the formation of public policy through our interactions with Treasury, ASIC, APRA, ACCC, ASX, ACNC and the ATO.

Our activities in this area

Governance Institute members have a strong interest in digital technology policy and take the governance and risk management of cyber security and data protection in all sectors very seriously. As a membership organisation, we have long advocated for digital transformation and modernisation in many areas of corporate regulation, including supporting virtual and hybrid AGMs, digital document execution, digital shareholder communications, and the introduction of Director Identification Numbers. Many of our members are working as governance and risk professionals in a range of organisations that are part of or connect with the digital economy, from the largest listed companies responsible for critical infrastructure to small businesses and not-for-profits. They are experienced in considering the industry and economy-wide implications of cyber security, technology governance, and digital transformation.

Governance Institute is a founding member of the ASX Corporate Governance Council, which produces the leading Australian statement on corporate governance, the Corporate Governance Principles and Recommendations. Recommendation 7.2 of the most recent edition explicitly acknowledges the importance of an organisation's risk management framework dealing adequately with cyber-security risk.[1] We strongly supported this inclusion. While the Corporate Governance Principles and Recommendations are directed at listed entities, they influence the governance practices of Australian organisations of all types and in all sectors.

[1] ASX 2019, *Corporate Governance Principles and Recommendations 4th Edition*, p. 27.

We also produce a range of thought leadership and industry guidance in this area. In 2020, we collaborated with CSIRO Data61 to compile a report on digital trust, which found cybercrime was one of the top two issues of concern to respondents.[2] We also published a report in 2020 that identified cybersecurity, artificial intelligence and digital disruption as key trends likely to impact on risk management professionals by 2025.[3] In partnership with Lexis Nexis, we recently released a whitepaper on cyber security.[4] We regularly contribute to a range of consultations on digital themes including Australia's 2020 Cyber Security Strategy and the Digital Australia Strategy 2030. Governance Institute of Australia also contributes to the international debate on cyber security in its capacity as a division of The Chartered Governance Institute (CGI), an international body with over 30,000 members worldwide.

Executive summary

- Governance Institute members welcome the opportunity to make this submission on the critical issue of cyber security. We acknowledge the overall policy objective is to strengthen Australia's national cyber resilience. Our members consider it is vital that governments, businesses, academics, civil society, and the community work collaboratively towards this aim to ensure Australia is a leading digital economy. They recognise cyber security threats are a significant and escalating risk to all sectors of the economy.

- Given the expertise of our members, we have targeted our comments at *Chapter 4: Governance standards for large businesses*. Our members agree that cyber security is and should be a governance and risk management priority for large Australian businesses and that it is appropriate to encourage organisations to consider cyber security through a broader assessment of governance, risk management and culture rather than taking a purely technical approach.

- We welcome the Government's stated intention to minimise regulatory burden. The challenge for Government in this policy development process is to strike an appropriate balance between supporting the boards of Australian large businesses to increase their cyber security resilience, posture, and awareness without unnecessarily increasing regulatory compliance burden in what is an increasingly complex area.

- We support in principle a voluntary governance standard for large businesses, provided it is well-designed, well-targeted and fit for purpose, and noting that many sectors and entities are already heavily regulated in this area.

- We encourage the Government to continue to support Australian organisations of all kinds through policy initiatives that go beyond minimum compliance standards and that encourage and support a capability uplift in all sectors, not just large for-profit businesses.

Recommendations

Recommendation 1A: Government co-designs with industry a voluntary governance standard that is well-designed, well-targeted and fit for purpose.

[2] Data61 and Governance Institute of Australia 2020, *Digital Trust: Corporate awareness and attitudes to consumer data*, p. 13.
[3] Governance Institute, 2020, *Future of the Risk Management Professional*, p. 19.
[4] Lexis Nexis and Governance Institute of Australia 2021, *Finding Certainty In A Time Of Zero Trust: Key issues from across Australia's cyber security landscape*.

The consultation paper makes a compelling case for change. As Governance Institute has acknowledged, cyber risks 'are omnipresent for businesses of all sizes today' and we consider effective management of cyber risk to be a marker of good governance.[5]

In our members' experience large Australian businesses have rapidly increased their cyber resilience, posture and awareness in recent years. This has been particularly apparent since the COVID-19 pandemic, and the boards of large Australian businesses are increasingly aware of cyber security, data protection, privacy, and related issues. Ransomware attacks, data sovereignty, the risks associated with widespread use of cloud services, and many other related topics are frequently discussed at our policy committee meetings. These are clear and present themes on the minds of governance and risk management professionals across Australia and on the agendas of the boards they support.

However, we acknowledge there is a role for government to encourage further enhancement. Governance and risk management practices in this area are continuing to develop and mature in response to rapid technological change and a constantly evolving threat environment. Our members agree it would be helpful for Government to lead, in consultation with industry, on the development of a voluntary, governance standard on cyber security. If appropriately designed, this standard would encourage less resilient organisations to adopt the better governance and risk management practices of their more developed corporate peers, and clearly communicate to industry public expectations on strong cyber security.

We strongly agree with the consultation paper that the standard should be voluntary, not mandatory, to reduce regulatory compliance burden.

A key challenge for the drafting minimum governance requirements on cyber security is that it will be an attempt to 'hit a moving target' – and one that is moving at exceptionally high speed. An example is the evolution of the Australian Signals Directorate's 'Top Four', originally released in 2011, which was updated in 2017 to the 'Essential Eight' in response to rapidly evolving threats, and then further updated in July 2021.

To meet its aims, our members consider that a voluntary governance standard would, at a minimum, need to be:

- principles based not prescriptive
- focused at a high level on governance and risk management, without delving into operational or overly technical matters
- sufficiently flexible and adaptable to account for wide variance of technology use and maturity levels across the sectors, risk profiles and access to cyber security resources of entities falling within the definition of 'large business'
- sufficiently broad so as to be capable of remaining relevant in the face of rapid changes in the cyber security environment without the need for constant revision, and
- general enough to encompass both existing and rapidly evolving threats and best practice.

The standard should be informed by existing principles, standards and regulation already in place in Australia and in other jurisdictions.

When developing the content of the standard, issues to consider include: context around the available evidence on comparable costs and benefits of cyber security investment, including reputational damage arising from breaches compared to investment in prevention and preparedness. A further consideration is articulating the importance of continuously assessing and increasing maturity levels in response to the rapid pace of change in this area, as well as providing guidance on the expected skills and competences for boards and individual directors.

Governance Institute members would be pleased to be involved in the co-design process.

[5] Governance Institute 2020, *Good Governance Guide: Cyber security*, p. 1.

Recommendation 1B: Use the voluntary standard to reduce regulatory burden and promote a consistent approach to cyber security across government.

A key principle of good policy making is that the cost burden of new regulation is offset by reductions in existing regulatory burden.[6]

Our members have identified a wide array of legislative obligations, voluntary industry standards and potential future regulation that may already apply to large Australian businesses in this area, and which are administered by a wide array of Government departments, regulators, agencies and industry associations – see Figure 1 below.

Figure 1 – Overview of Australia's increasingly complex digital regulatory framework

Scheme / framework / standard	Oversight body	Purpose	Status
Security of Critical Infrastructure Act 2018 (Cth)	Department of Home Affairs / Australian Signals Directorate	To protect Australia's critical infrastructure from cyber security and other threats.	In force, soon to be expanded
Privacy Act 1988 (Cth) and its Australian Privacy Principles	Attorney-General's Department	To provide the basis for nationally consistent regulation of privacy and the handling of personal information.	In force, under review
Consumer Data Right (CDR) Privacy Safeguard Guidelines	ACCC / Office of the Australian Information Commissioner	To give consumers greater access to and control over their data.	In force, soon to be expanded
Notifiable Data Breaches (NDB)	Office of the Australian Information Commissioner	To ensure individuals can take steps to protect themselves in the event that their personal information is compromised in a data breach.	In force
CPS 234 Information Security	APRA	To ensure APRA regulated entities take measures to be resilient against information security incidents (including cyberattacks) and provides that the boards of these entities are ultimately responsible for information security.	In force
Cyber resilience good practices[7]	ASIC	Guidance for all organisations to improve their cyber resilience preparedness.	Current, non-binding

[6] Department of the Prime Minister and Cabinet 2016, 'Regulatory Burden Measurement Framework', Guidance Note, viewed 12 August 2021, https://www.pmc.gov.au/sites/default/files/publications/regulatory-burden-measurement-framework.pdf

[7] ASIC 2021, viewed 12 August 2021, Last updated 30 March 2021, https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/

Corporations Act 2001 (Cth)	Treasurer, ASIC, APRA	Regulate Australian companies, including directors' duties.	In force
Australian Financial Services Licence (AFSL) cyber resilience obligations under Corporations Act sections 912A(1)(c) and (ca) and 961L	ASIC	ASIC Report 555 and Report 651 on the cyber resilience of AFSL holders and its Federal Court proceedings against an AFSL holder in 2020 for failing to have adequate cyber security systems under section 912A indicate ASIC is willing to pursue regulatory action in this area.	In force
Part 6 and 13 of the *Telecommunications Act 1997* (Cth)	Department of Infrastructure, Transport, Regional Development and Communications	Use, storage, handling and disclosure of personal information obtained by certain bodies during supply of telco services.	Mostly superseded by Privacy Act
Essential Eight	Australian Signals Directorate	Baseline cyber security strategies for all organisations. Mandatory for all PGPA Act entities.	In force
Cyber Security Principles	Australian Cyber Security Centre	Guidance for industry on how to protect systems and data from cyber threats.	Current, non-binding
ASX Corporate Governance Principles and Recommendations, 4th edition – Recommendation 7.2	ASX Corporate Governance Council	Guidance for listed companies on managing cyber risks.	In force, mandatory reporting for listed companies
ISO/IEC 27000-series	International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)	Best practice recommendations on information security management.	In force, non-binding
Principles for Board Governance of Cyber Risk	World Economic Forum	Guidance for company directors.	Current, non-binding
Ransomware notification scheme	N/A	Combat the growing threat of ransomware.	Reportedly under consideration, not legislated

Our members see the proposed co-design drafting process as an opportunity to harmonise these varying obligations, rules and standards into a cohesive standard that reduces duplication and leverage what is already in the market, including in other jurisdictions. We must avoid a scenario where cyber security regulation across sectors of the Australian economy is fragmented and burdensome. Any proposal for a voluntary standard should be assessed in this context. If a voluntary standard is implemented that adds to rather than reduces regulatory complexity, this will be counterproductive to the aim of strengthening the cyber resilience of large businesses.

As shown in Figure 1, there are a number of different and overlapping oversight bodies and frameworks active in digital regulation. Our members consider it is important for the standard to

find a ‘home’ within an appropriate framework and under the authority of an appropriate regulator or agency with the relevant areas of expertise. This will require careful coordination by Government, having regard to the various overlapping areas of policy, areas of law, the various programs of work currently underway by different areas of government, and the wide array of regulated entities and affected stakeholders.

Recommendation 1C: Consider extending the voluntary standard to public sector entities.

Many of the arguments in the consultation paper about cyber resilience and preparedness apply equally, if not more so, to public sector entities. Figure 1 illustrates the heavy digital and cyber security regulation to which large Australian businesses in the private sector are, to varying degrees, subject. By contrast, public sector entities constituted under Commonwealth, state and federal legislation are often subject to a far lesser degree of regulation in this area. We note that the proposed changes to the Critical Infrastructure Act may capture some of these entities. However, applying the voluntary standard to public sector entities to which the Critical Infrastructure Act does not apply, and involving these entities in the drafting process, may help to achieve the broad policy aim of strengthening Australia’s cyber resilience in all sectors.

Recommendation 2: Promote more than minimum compliance with the governance standard.

Our members would want to avoid a scenario where large Australian businesses do no more than comply with what may be perceived to be minimum requirements in the new standard, without any genuine attempt to improve cyber resilience.

In evidence to a Parliamentary Joint Committee earlier this year, as part of an inquiry into the new Critical Infrastructure Bill, the Victorian Safety Commissioner warned that a ‘checklist’ approach to cyber security based around compliance with minimum standards can become little more than ‘security theatre’ and that a better approach is to focus on promoting ‘security awareness’ and ‘capability building’.[8]

For these reasons, our members see a role for Government in continuing to promote capability building and increased maturity by continuing to provide advice, cyber security intelligence sharing, and initiatives that provide direct support to industry. Our members note with approval the funding committed by the Government for a Digital Directors Training package in the 2019-20 Federal Budget, and the expansion and enhancement of the Australian Small Business Advisory Services program as part of the Digital Economy Strategy 2030 in the 2021-22 Federal Budget. We encourage the Government to continue to develop direct support measures for digital capability building in large businesses, as an alternative to increased regulatory compliance burden.

In addition, Government should continue to consider other impediments to the cyber resilience and posture of Australian organisations in all sectors. For example, our members consider that it can be difficult for boards to attract directors with sufficient digital technology skills, and that it is difficult or costly to employ employees or hire consultants with necessary expertise – especially for smaller organisations. This skills gap has been exacerbated by Australia’s border closures and migration limits during the COVID-19 pandemic and is a key area where Government could provide assistance to industry.

Recommendation 3: Avoid an issues-based approach to directors’ duties.

[8] Hansard 2021, Parliamentary Joint Committee on Intelligence and Security, public hearing 11 June, p. 15-16.

The consultation paper acknowledges that directors' duties extend to cyber security, but argues they are not sufficiently specific to cyber security expectations and 'focus on protecting the interests of shareholders, rather than customers'.[9]

Governance Institute urges a cautious approach to expanding director liability in response to specific emerging issues. Our members consider the range of existing directors' duties and obligations under the Corporations Act, the common law and company constitutions (where applicable) to be sufficiently broad to adequately cover care and diligence obligations relating to cyber security. In a different context the recent opinions of barristers Noel Hutley SC and Sebastian Hartford Davis advise that in order to comply with existing duties, diligent company directors ought to be considering climate change risks and that directors' existing duties are sufficiently broad to include climate change risks.[10] Our members would argue cyber security risks are similar and directors existing duties already incorporate these risks.

The standard expected of directors of Australian entities is already high by international comparison, there appears to be a trend towards imposing greater personal liability on directors, and recent cases suggest that Australia's corporate regulators are increasingly willing to pursue civil and criminal action against directors. Analysis by Allens Linklaters commissioned by the Australian Institute of Company Directors (AICD) in 2019 found that director liability in Australia is 'in many regards, uniquely burdensome' compared to the legal systems of Canada, Hong Kong, New Zealand, the United Kingdom and the USA, including 'a relatively broad range of subject matter'; the application of criminal liability to directors 'relatively liberally'; and civil and criminal penalties that are 'relatively harsh'.[11]

Our members also note that the cost of Directors' and Officers' (D&O) insurance has increased substantially in recent years in all sectors. This cost increase has been directly observed by our members who are company secretaries, as board-related costs frequently sit in the company secretary's cost centre. Further expansion of director liability may risk additional cost escalation in the D&O insurance market.

If you wish to discuss any of the issues raised in this letter, please contact me or Catherine Maxwell.

Yours faithfully,

Megan Motto
CEO

[9] Department of Home Affairs 2021, *Strengthening Australia's cyber security regulations and incentives: An initiative of Australia's Cyber Security Strategy 2020*, consultation paper, p. 15.
[10] The Centre for Policy Development 2020, *Climate Change and Directors' Duties: Supplementary Memorandum of Opinion*.
[11] AICD 2019, *Criminal and Civil Frameworks for Imposing Liability on Directors*, p. 2.