THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:JBml280825

28 August 2025

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

By email: natalie.cooper@lawcouncil.au

Dear Dr Popple,

HORIZON 2 OF THE 2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY

Thank you for the opportunity to contribute to the Law Council of Australia's submission in response to the Department of Home Affairs' Discussion Paper on Horizon 2 of the 2023-2030 Australian Cyber Security Strategy (**Horizon 2 Paper)**. The Law Society's Privacy and Data Law Committee contributed to this submission.

We mainly focus on Shield 1 and Shield 4 of the Horizon 2 Paper, as highlighted by the Law Council's Memorandum.

General comments

In our view, a holistic and coordinated approach is needed to address what has become a key and endemic concern for all Australians due to the frequency and ubiquity of cyberattacks and data breaches across the public, private and other sectors. We are concerned that the Horizon 2 Paper reflects the current piecemeal regulatory approach. We suggest that an effective cyber security requires a coordinated response from all levels of government, particularly considering the significant social and economic costs associated with cyberattacks and data breaches.

The considerations in the Horizon 2 Paper could be assisted by the development of practical and effective measures to uplift cyber security and to protect vital infrastructure and networks from cyberattacks. We set out below some examples of some practical measures.

Robust cyber security to be mandatory

In our view, given the detriment caused by cyberattacks and data breaches on individuals and organisations, including the costs incurred, cyber security management should no longer be considered optional. We suggest it is necessary to require organisations to implement robust cyber security measures, substantiated by relevant minimum standards and codes that have the effective force of regulations. Arguably, the Office of the Australian Information Commissioner (**OAIC**) has taken a step in this direction with the Australian

Information Commissioner's Notice of Filing in the Federal Court against Medibank Private,[1] and its broad recommendations regarding minimum standards for larger corporate organisations.[2] However, in our view, those recommendations should be given practicable focus and converted into enforceable standards. The implementation of such standards could also form the basis of a defence to regulatory sanctions or act as a benchmark for obtaining cyber insurance compensation.

Mandatory cyber security insurance

We suggest that the Australian Government considers establishing mandatory cyber security insurance for all organisations dealing with personal information, regulated centrally by a cyber security authority. Mandatory cyber security insurance could operate in a manner similar to State Governments' mandatory Compulsory Third Party personal injury insurance on cars, offering a basic level of data breach coverage, along with fines levied against organisations that have failed to obtain insurance or meet minimum cyber security standards. The Government may wish to consider the UK Information Commissioner's Office (**ICO**)'s Data Protection Fee (**DPF**)[3] model as a possible funding model for a mandatory cyber security insurance regime. If the Australian Government were to pursue an ICO-style funding model, a portion of the DPF equivalent could be allocated to the proposed cyber security authority's operations, including relevant investigations and rectification efforts.

Centralising and harmonising responses to cyberattacks and data breaches

We suggest that establishing a federal cyber security authority may assist the Australian Government to centralise and coordinate responses to cyberattacks and data breaches. As in the case of the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI**), legislative authority could flow from section 51(v) of the Australian Constitution[4] and apply to all cyberattacks occurring through telephonic or digital means. We suggest the recent reforms to the *Privacy Act 1988* (Cth), in particular, sections 26X and 26XB(4), are a step in that direction. Those sections provide the Attorney-General with powers to make Eligible Data Breach Declarations that effectively suspend Australian Privacy Principles (**APP**) protections for up to a year (s 26XA(c)) where there are confirmed or suspected cyberattacks. These Declarations would enable the Australian Government to share personal information with State, Territory and Australian law enforcement, banks, telecommunications providers, while containing the damage occasioned by cyberattacks.

In our view, a cyber security authority could build on those new powers under the privacy reforms in a more coordinated fashion, focusing on privacy-by-design principles and working with the public, private and non-government sector to protect and recover from cyberattacks. A cyber security authority could also undertake

[1] Notice of Filing, Australian Information Commissioner v Medibank Private Limited (2024): https://www.oaic.gov.au/__data/assets/pdf_file/0025/221974/Australian-Information-Commissioner-v-Medibank-Private-Limited-concise-statement.pdf.
[2] See Annexure B, Australian Information Commissioner v Medibank Private Limited concise statement (2024) 9-11: https://www.oaic.gov.au/__data/assets/pdf_file/0025/221974/Australian-Information-Commissioner-v-Medibank-Private-Limited-concise-statement.pdf.
[3] UK Information Commissioner's Office, 'Guide to the data protection fee': https://ico.org.uk/for-organisations/data-protection-fee/data-protection-fee/.
[4] Commonwealth Of Australia Constitution Act, s 51(v): 'The Parliament shall, subject to this Constitution, have power to make laws for the peace, order, and good government of the Commonwealth with respect to … Postal, telegraphic, telephonic, and other like services.'

investigations regarding the adequacy of cyber security measures, among other matters. We acknowledge that the proposal to establish a new cyber security authority would require reconsideration of the operation, legislative remit and government commitment to resourcing for current regulators. As noted further below in our submission, we consider the current piecemeal regulatory approach, where there are multiple regulators enforcing different cyber security or data-related obligations for different entities, does not assist with an outcomes-focused model that is effective in protecting data and containing breaches. Instead, organisations are often subject to multiple layers of reporting obligations when agility and centralisation of response are needed during a cyberattack or data breach. For example, the Cyber and Infrastructure Security Centre regulates entities with critical infrastructure under SOCI; OAIC regulates APP entities and manages the Notifiable Data Breaches scheme; the Australian Securities and Investments Commission (**ASIC**) and the Australian Prudential Regulation Authority (**APRA**) both pursue action against their regulated entities for failings in different cyber-related obligations.

Considering the significant regulatory burden imposed by the increasing scale of cyberattacks, which affect millions of Australians and result in substantial rectification costs, we suggest that a different approach may be warranted.

A feature of the centralisation of response may be for the State, Territory and (by extension) Local Government authorities to refer their data breach response powers to the proposed cyber security authority. Such a referral would have the benefit of developing a national or unified approach to cyber security and data breach responses.

If referral of powers is not possible (for example, for constitutional reasons), we suggest that breach response frameworks should be harmonised across Commonwealth, State and Territories, for example, through an intergovernmental agreement, similar to the model adopted to harmonise Work, Health and Safety laws.[5]

Attracting cyber talent

Noting that the Horizon 2 Paper calls for a whole-of-economy-and-nation approach,[6] including making Australia a top destination for cyber security talent and a leader in cyber research,[7] we suggest the Australian Government could consider using various levers to attract cyber security professionals to work and live in Australia, e.g. training and transition pathways for graduates trained in cyber security; skilled migrant pathways; tax rebates for employer engaging these professionals, or tax incentives for cyber security talent to settle in Australia.

Government to be model for cyber security

We suggest that just as the Australian Government is a Model Litigant, the Australian Government should also be a model in setting the 'gold standard' for cyber security. Given the number of online services storing personal and health information, including MyGov and My Health Record, the public's trust in the digital

[5] https://www.safeworkaustralia.gov.au/development-model-whs-laws.
[6] Department of Home Affairs, *Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy* (2025) 1.
[7] Ibid.

environment will be undermined if the Australian Government does not lead by example in its cyber security infrastructure and messaging.

Shield 1: Strong businesses and citizens

5. What could government do better to target and consolidate its cyber awareness message?

In our view, cyber awareness messaging from the government is useful for setting the expectation that cyber security is not optional. Everyone needs to be cyber aware, and that no small business is too small to be a victim of cyberattacks. In education materials, analogies may be drawn using easily understood images, e.g. that not having cyber security is akin to leaving one's front door open. Such materials should also be appropriately segregated, having regard to the level of digital and cyber literacy of the target audience, and the context. For example, messaging to technical IT professionals would be different to sales professionals.

9. What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs?

We consider that if the Government invests resources into cyber security, industry will follow that example.

For not-for-profit and charity organisations, we suggest the government offers tailored packages such as checklists, to alleviate the burden on volunteer boards. This is particularly important because of the large amount of personal information these organisations often hold.

We suggest, as a matter of best practice in relation to cyber security:

- that businesses align with the principles and guidelines outlined in the *Information Security Manual*[8] developed by the Australian Signals Directorate and Australian Cyber Security Centre, as a baseline;
- that businesses consider aligning their cyber security posture and standards to be equal to or greater than that of their most secure client, for example, clients who are regulated under the SOCI or by the APRA;
- that businesses consider aligning with ISO/IEC 27001, the international standard for information security management systems;[9] and
- where necessary, ensure that all suppliers, not just information-technology suppliers, understand the business's cyber security standards and expectations.

16. Which regulations do you consider most important in reducing overall cyber risk in Australia?

We suggest that regulation that protects data and compels behaviour should be easy to understand and comply with and contain meaningful enforcement or penalty mechanisms. In our view, current regulations are not good examples of these principles.

[8] https://www.cyber.gov.au/sites/default/files/2024-12/Information%20Security%20Manual%20%28December%202024%29.pdf.
[9] https://www.iso.org/standard/27001.

We note that there is no general duty for a company to implement cyber security or data protection systems under Australia's corporations legislation. In our members' experience, currently, directors have been largely able to avoid the consequences of cyber security failings through delegating 'cyber' matters to their employees, which does not create any incentive to act effectively on cyber issues.

However, Australian Financial Services License (**AFSL**) holders are 'required by law to have adequate cybersecurity risk management systems in place'[10], and the ASIC has been actively litigating AFSL holders for cyber security failings.[11] APRA-regulated entities are also subject to specific data protection obligations.[12] We query why only limited categories of entities are held to this standard despite other industries holding substantial amounts of data and personal information, and often with less resources to protect that information.

The Australian Government may consider adopting the requirements for AFSL holders as a new corporate standard. It might also consider sending a clear signal to companies that data and privacy security are part of 'doing business' and not optional. We suggest that this could be included as a director's duty as part of section 181 of the *Corporations Act 2001* (the duty to act in good faith and the best interests of the company). It is in the best interests of corporations, and wider society, to have robust and best practice data and privacy security in place. If this new duty were included, section 180(2), the business judgement rule, and section 189, already contain defences for a director to raise, for example, that they obtained and implemented expert advice to inform themselves.

In our view, much like Work Health and Safety laws, enshrining cyber, data and privacy security at the board level is essential to ensure action takes place – especially where it is a societal expectation.

18. What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, consumer energy resources (CER) and operational technology?

As mentioned in our response to question 9, we suggest alignment with ISO/IEC 27001, the international standard for information security management systems.

We commend the actions taken by Estonia in offering e-services and e-governance frameworks as a good case study for Australia.[13]

---

[10] See, for example, comments by ASIC Chair Joe Longo in ASIC Media Release, 13 March 2025: https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-035mr-asic-sues-fiig-securities-for-systemic-and-prolonged-cybersecurity-failures/.

[11] See, for example, *ASIC v RI Advice Group Pty Ltd* [2021] FCA 1193; ASIC v Fortnum Private Wealth Ltd (2025); ASIC v FIIG Securities Limited (2025).

[12] Refer to Prudential Standard CPS 234: Information Security: 'This Prudential Standard aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyberattacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats.'

[13] e-Estonia, 'We have built a digital society and we can show you how': https://e-estonia.com/; 'Building a digital society': https://e-estonia.com/solutions/.

Shield 4: Protected critical infrastructure

35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

In our members' experience, the regulatory burden for reporting often proves too onerous or rigid for organisations during a cyber breach, where quick and agile responses are required.

We consider that current regulations are not outcome focused. The layers of reporting obligations under the SOCI, *Privacy Act 1988* (Cth), and other legislation can prove confusing and costly for organisations, and even more burdensome for organisations that also have international reporting obligations. Instead of concentrating their resources on quickly responding to the breach, resources are often diverted to navigating the regulatory landscape.

As noted in our general comments, we suggest a coordinated, agile approach led by the Australian Government needs to be developed, rather than piecemeal or scattered regulations with separate regulators.

36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

We suggest implementing regular audits of critical infrastructure to motivate best practice. For example, a cyber drill may be very beneficial in identifying the strengths and weaknesses in the infrastructure. To further incentivise organisations, we suggest considering the policy option of reducing insurance premiums if cyber drills are performed at regular intervals.

37. How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

We suggest the Government could support the private sector by ensuring consistency and education across government entities, especially among procurement officers and decision makers (not just its technical experts), so that there is a shared and consistent knowledge. When supplying goods or services to Government, businesses may face the challenge of inconsistent positions between Departments. Further, in our members' experience, businesses may sometimes have a better understanding of the technical security requirements, certifications, and controls than the Government's representatives. This not only leads to substantial waste in the contracting process, but also lead to misaligned or poorly scoped projects, or projects with compliance costs that were unnecessary (for example, because a procurement officer did not understand which of the default standards included in the Government's template contracts could be safely removed).

In our view, the Government should also ensure that when selecting suppliers for any of its Panels (including for its legal services, technical services, or other professional consulting panels), it should test panel applicants for their understanding of Government Frameworks, rather than simply requiring contractual compliance on paper. Our members have noted it is routine for Government to include a 'shopping list' of standards and controls (for example, default terms the Government's Digital Marketplace Panels) but these are treated as a box ticking exercise, with no real validation undertaken.

Simultaneously, the Government can continue supporting the work of the Australian Signals Directorate in terms of thought leadership and guidance, so that businesses are encouraged to align to a national standard. The Protective Security Policy Framework (**PSPF**)[14] provides a good framework, and in the absence of any other national framework, PSPF may be the best option for Australian businesses to align to. However, we acknowledge not all businesses will have the resources, time or technical expertise to comply with the PSPF.

3.6 Shield 6: Strong region and global leadership

46. Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

We acknowledge that while sanctions might be effective tools against state actors, many malicious cyber actors will not be affected by such, or their commercial gain from such activities far outweighs any detriment – especially if they are never identified by name, or they belong to a State that Australia has already sanctioned, and are therefore unconcerned with sanctions.

In some cases, attributions are more likely to be considered as 'status' points for threat actors, and are likely to encourage this unwanted behaviour (as we understand many threat actors trade on a reputation built on attributions for their past activities).

Information sharing and advisories can assist if they are informative, have clear action items, and are gazetted to persons who should know (or otherwise, if there is a method for such persons to subscribe to).

In our view, cyber diplomacy as a concept is unlikely to be useful. As above, where a threat actor is taking such actions because they are either taking directions from a State or they have a vested commercial interest, there is little 'diplomacy' to be had. From a pragmatic perspective, Australia needs to uplift its practices across business, government and community to be less of a target; and equally, it may need to consider what national level responses it should take to being attacked by another nation State.

As a non-hostile deterrence, the Australian Government could institute standards for data redundancy, i.e. enshrining best practice for data redundancy in law. Many ransomware events are perceived threats due to the loss of the compromised data, in addition to the potential release or exposure of it. However, if data loss is mitigated or entirely avoided due to enforced data backups, then this would decrease the level of concern for those involved. It is likely that by enshrining data redundancy measures in law, insurers would also follow suit, and while this may have a cost impact on business, it would lead to a discernible shift in practice.

[14] https://www.protectivesecurity.gov.au/.

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

We suggest uplifting domestic capability in cyber security. We also suggest the Government continues to support the work of the Department of Foreign Affairs and Trade in the Pacific and with ASEAN countries in continuing to develop cyber security legislation and supporting hard infrastructure.[15]

If you have any queries about the items above, or would like further information, please contact Mimi Lee, Policy Lawyer, on 02 9926 0174 or mimi.lee@lawsociety.com.au.

Yours sincerely

Jennifer Ball

Jennifer Ball
President

[15] Department of Foreign Affairs and Trade, 'Pacific Cyber Security Operational Network': https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/pacific-cyber-security-operational-network-pacson.