Queensland Law Society

Law Society House, 179 Ann Street, Brisbane Qld 4000, Australia
GPO Box 1785, Brisbane Qld 4001 | ABN 33 423 389 441
[redacted] | [redacted] [redacted] qls.com.au
Office of the President

25 August 2025

Our ref: [KS:PDTIPS]

Dr James Popple
Chief Executive Officer
Law Council of Australia
Level 1, MODE3
24 Lonsdale Street
Braddon ACT 2612

By email: [redacted]

Dear Dr Popple

Developing Horizon 2 of the 2023–2030 Australian Cyber Security Strategy (the Strategy)

Thank you for the opportunity to provide feedback on the development of Horizon 2 of the 2023–2030 Australian Cyber Security Strategy – Policy Discussion paper.

This response has been compiled with input from the QLS Privacy, Data, Technology and Intellectual Property Law Committee.

QLS emphasises that in implementing Horizon 2 of the Strategy, support must be provided to small businesses who are increasingly under pressure to manage compliance and risk associated with cybercrime, privacy (and data security), ESG and other reporting obligations.

The Australian Cyber Security Centre's 'Cyber security checklist for small businesses' recommends speaking to an IT professional about securing networks and implementation of Maturity Level One of the Essential Eight. However, resource constraints for micro to small businesses means in many cases those businesses will need to engage third parties to implement technical requirements, placing them at a disadvantage to those businesses with access to internal IT professionals.

While a maturity model approach is necessary when dealing with businesses with diverse threats and resources to face them, Essential Eight is not necessarily the best starting point for many smaller entities. It has a heavy focus on technical controls, including some which can be expensive to implement. Other frameworks are emerging[1] which may be a better starting point for micro to small business.

[1] Such as Dynamic Standards International (DSI)'s SMB 1001

Regulatory impact analysis – small business

As such, the government must endeavour to control costs as regulation is increasingly applied to small businesses. This is critical in a context where the financial impact on small businesses as a result of cybercrime continues to increase.

We support a strengthened focus on providing small business clear and low or no cost cyber standards coupled with implementation and targeted support. We strongly suggest that these initiatives be co-designed with experts who have experience as owners of and suppliers to genuinely small business (including sole operators). This should go beyond final stage consultation and should ensure that any regulation and guidance is designed from the ground up to be responsive to the needs of small business.

QLS would also welcome a regulatory impact analysis with respect to any specific actions and initiatives which are proposed as part of this process, to ensure the next stage of the government's response adequately considers the impact on small businesses and allocation of sufficient government funding to support uptake and ongoing compliance. The analysis should consider the impacts on small businesses of different sizes, types, and location.

Supply chain pressures

The policy discussion paper recognises that small and medium sized businesses form part of the critical infrastructure supply chain.

Our members similarly observe that requirements are ultimately being pushed down the supply chain. For example, critical infrastructure entities are required to comply with various standards as well as enhanced security standards. Although these requirements are aimed at larger businesses, they are often pushed down the supply chain, requiring small businesses to meet them.

In addition, the *Privacy Act 1988* (Cth) (**the Act**) allocates risk as between the principal and contractor, even if the contractor is outside the scope of the Act. Consequently, the issue arises as to who holds the data and subsequently who has the responsibility when the act of an agent is deemed to be the act of the principal. Smaller businesses may have significant exposure in this respect including the potential for regulatory and civil penalties.

Encouraging up-take

Safe harbour programs, free training and low cost certification should all be considered in preference to top-down regulation and shifting liability to small business.

Many small enterprises struggle to obtain expert assistance as the cost of performing gap analysis, educating the customer then performing necessary work on a less than ideal network can be unattractive to providers who are already struggling to service existing clients. A well understood program "in a box" that can be tailored to individual sectors would lower the cost of delivery significantly.

Unintended impacts for small business and the regions

Our members have reported that one of the unintended impacts of the current framework, is that larger businesses are having to carefully rethink engaging small businesses due to third party vendor risks.

Members also report that procurement practices at a government level mean that small, regional and remote businesses are often ineligible to win some government contracts as they simply

do not have access to the necessary resources. Some regions will not have sufficient local capability in the ICT sector. These impacts are more acute in the regions meaning that less businesses in regional and remote areas will succeed in acquiring the work.

Accordingly, the government must also consider supporting small, regional and remote businesses by subsidising programs they must participate in to meet any pre-qualification requirement to tender for government work.

If you have any queries regarding the contents of this letter, please do not hesitate to contact our Legal Policy team via policy@qls.com.au or by phone [redacted]

Yours faithfully

[redacted]

Genevieve Dee
President