27 August 2021

Technology Policy Team
Department of Home Affairs
Belconnen ACT 2617

Via upload.

Dear Sir/Madam

Strengthening Australia's cyber security regulations and incentives

AFMA is pleased to make comment on the Department of Home Affairs' *Strengthening Australia's cyber security regulations and incentives* consultation paper. A number of AFMA's members are already captured as critical infrastructure providers, and many more would be likely captured by some of the initiatives the paper proposes.

It is important that Government and industry align and coordinate their efforts and work together in building cyber aware businesses in our digital economy, and accordingly we welcome the Department of Home Affairs' consultation on these issues. AFMA is strongly supportive of the aim of the initiative to make Australia's digital economy more resilient to cyber security threats. This is an entirely appropriate and timely aim and there is little doubt that the prudent deployment of Government resources can assist the business community build its resilience.

The most effective approach is likely an accommodative one with a clear focus on helping business build improvements where they are required. We remain concerned that framing the national economy's cyber resilience as largely a consumer law matter may not be the optimal approach. It may feed into a slower more costly and punitive regulatory infrastructure that is unlikely to be the most effective way to drive a rapid raising of standards.

AFMA's main concern in responding to this consultation is to express our strong support for a voluntary cyber governance standard. We believe a voluntary approach is the most efficient and effective approach to improving outcomes in a market economy.

We trust our comments below are of assistance.

Yours sincerely

Damian Jeffree

Senior Directory of Policy

Governance standards

AFMA's focus in responding to this submission is on the proposals around governance standards for large businesses. Governance is the right place to start as getting the governance right is the best chance to lead to sustainable and substantive security outcomes on the ground. We are strongly in support of common standards in relation to cyber governance but stress the need to avoid duplication. The Government should ensure harmonisation of regulatory requirements not only within specific sectors but also across sectors to prevent increasing compliance costs outweighing benefits.

AFMA strongly supports voluntary governance standards co-designed with industry (Option 1) for larger businesses. Voluntary standards are powerful, and even when not mandated will effectively get picked up as the reference benchmark by various regulators, and the market at large. The definition of large business should be clear to ensure medium to small businesses are protected from the application of these standards to them notably in relation to director's duties.

In a market-based economy firms will face significant economic pressures to meet expected standards.

Voluntary standards can be kept more agile and responsive as their purpose is to inform and support rather than act as a means to prosecute actions against companies. The prosecutorial use of standards requires slower, less responsive processes for their change and updating given the risk of creating unfair enforcement requirements on business.

A voluntary approach would fit in more readily with existing mandatory requirements (e.g. CPS 234) as it would allow businesses to determine the best implementation approach after weighing the costs and benefits. For those firms already caught as critical infrastructure providers the standard should not conflict or add additional expectations above those expected under the *Security Legislation Amendment (Critical Infrastructure) Bill* 2020 or existing mandatory standards. It should be consistently applied across all industries.

Under a voluntary arrangement we would still encourage the inclusion of a transition period to enable businesses to ensure compliance.

Adoption of best cyber security practice starts with a strong understanding of the cyber security risks posed to businesses. As such AFMA encourages Government to complement the voluntary standard with adequate awareness campaigns and enhanced cyber security educational resources to make it easier for businesses to understand and adopt the standards. The campaigns should explain cyber risk to businesses in simple terms and provide guidance on fundamental steps that businesses can take to secure their organisations from these risks. They should provide easy-to-follow advice that considers the not unlimited time and resources of businesses.

AFMA is cautious about Option 0 – Status quo. While many businesses have advanced cyber governance practices, particularly in financial services, cyber security is a network challenge, and there are benefits in assisting all firms reach a common understanding of what is expected in relation to it. A general uplift in non-finance firms that are not already regulated (such as under APRA's CPS 234), would also be beneficial to financial firms as these firms connect to these businesses and have exposures to them as clients.

AFMA is strongly opposed to Option 2 – Mandatory governance standards for larger businesses. Mandatory standards are high cost and can direct significant energy towards exercises designed to evidence technical compliance as a defensive measure against regulatory action rather than keeping a clear focus on defending against cyber risks. As noted above mandatory standards are not as agile as voluntary standards due to their use in enforcement actions.

AFMA supports the view expressed in the consultation paper that the risk of poor regulatory settings and particularly overlapping mandatory standards is that regulatory burden makes it difficult for businesses to operate in Australia.

More generally and perhaps significantly mandatory standards risk changing the paradigm of government intervention in security governance for affected firms from a supportive and open engagement to a closed and defensive one. Businesses will be less inclined to share intelligence and lessons learned if it will increase their chance of prosecution.

We agree with the position noted in the paper that a mandatory standard would likely create significant overlap with the existing regulatory requirements both locally and internationally.

Minimum standards for personal information

The setting of technical requirements can impose high costs on businesses and should be considered within an international context. These costs include the implementation of expected controls and the assurance required to confirm adherence. For those subject to the Security Legislation Amendment (Critical Infrastructure) Bill 2020 this could add an additional level of implementation and potential for conflict with rules defined under the Bill. The level of OAIC oversight would need to be explored to confirm the expectation that costs are moderate and what costs the oversight will impose on business.

We would encourage consistency with existing cyber security requirements as well as the ACSC mitigation strategies, and assessment of impacts on compliance costs are of utmost importance if another enforceable code is to be introduced. Particular consideration should be given to the potential for requiring businesses to provide duplicative reporting to different government and regulatory agencies. This may constitute an unintended additional regulatory burden on businesses.

One option could be to include the minimum best practice approaches and controls within the voluntary governance standards such that businesses benefit from the guidance contained in the standards while continuing to have the flexibility of determining the best way to implement such best practice approaches and controls, commensurate to the size of their business, and the threats and risks faced.

We also note that an enforceable cyber security code would require consequential amendments to AP11 – security of personal information. This would require changes to existing procedures.