CESA
CONSUMER ELECTRONICS SUPPLIERS ASSOCIATION

AREMA

27 August 2021

Department of Home Affairs

https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers

Dear Sir/Madam

Joint Submission: Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper

The Consumer Electronics Suppliers Association (CESA) welcomes the opportunity to make a submission on the above Discussion Paper. CESA is the premier national, industry body in Australia representing the consumer electronics industry. CESA Members encompass the majority of global suppliers of consumer electronic products and thus, is a key stakeholder in the supply of smart (IoT) devices.

AREMA (the Air-Conditioning & Refrigeration Equipment Manufacturers Association of Australia) represents the interests of air-conditioning and refrigeration equipment manufacturers and importers active in the Australian market. AREMA members include leading companies involved is supplying over 80% of air conditioners to the Australian market. We work with government and industry on policy formulation and regulation to achieve the best outcomes for our members and the wider community.

General Comments

CESA/AREMA endorses the broad objectives of the proposed regulations to:

- incentivise businesses to invest in cyber security;
- set clear cyber security expectations, increasing transparency and disclosure,
- protecting consumer rights;
- seeking to reduce the social and economic impacts of cyber security incidents to Australia's digital economy and society; and
- encouraging businesses to better manage cyber risk and promoting 'secure by design' principles.

Specific Comments

Regarding specific issues raised in the Discussion Paper, of particular interest to our members are Chapter 6(Standards) and Chapter 7(Labelling). The following responses address the questions on these issues raised in the Paper:

Standards for Smart Devices

What is the best approach to strengthening the cyber security of smart devices in Australia?

We consider that if an evidenced based case demonstrating a net community benefit is made, then and only then, should an approach based on international standards and labelling schemes be considered. As Australia is largely dependant on the global supply of IoT devices, adoption of unique Australian standards and labels would add a significant cost burden on suppliers and ultimately consumers.

After the results of the UK regulations are known and are seen to be successful, then Australia could consider adoption of same regulations.

Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices?

- *If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?*
- *If not, what standard should be considered?*

ETSI EN 303 645 is the appropriate international standard to adopt. We consider the top three requirements of the standard to be adequate in the first instance as larger markets such as Europe and the UK have adopted or intend to adopt these higher priority principles. This approach would also limit the cost burden on suppliers and align Australia with international best practice.

Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

This issue would be up to Retailers to consider.

Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

If Australia introduced additional requirements to the UK the costs will be much higher. The international data in the paper would need to be re-examined depending on the additional requirements. We further endorse the need for industry consensus-based standards and the direct adoption and referencing of international standards.

Labelling for Smart Devices

Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

Australia should wait to see how mandatory notification of security support period works in the UK. The UK does NOT impose specific means such as physical labelling of the security support period. Also, the UK decided not to go with mandatory labelling.

Is there likely to be sufficient industry uptake of a voluntary label (Option 1) for smart devices? Why or why not?
If so, which existing labelling scheme should Australia seek to follow?
A voluntary star rating label would be unlikely to generate a significant industry uptake. Company policies vary substantially on this issue. As the Australian market for IoT devices is largely supplied by global offshore suppliers there would be little incentive for suppliers to adopt a specific label for the Australian market. If there was acceptance for such a label in larger jurisdictions, then perhaps it could be adopted here. A voluntary star rating may not work, especially when the star rating may give misleading information (although 4 stars only means the snapshot performance at the time of test)

Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?
As in the coming UK regulation, displaying the security support period on the website would be a great first step to improve Australia's cybersecurity. If the product sells very well, manufacturers are quite likely to extend such a period to continue to sell the product. Physical labelling may make it difficult for such extension. It should be kept digital/online for easier extension. However, security expiry could be problematic as it calls into mind planned obsolescence of appliances and does not fit well into the circular economy model because people would think their product becomes functionally useless after that expiration date.

Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?
No. Mobile phones already incorporate rigorous cyber security features in their design and have regular security updates sent by the manufacturer available for download. Consumers are already aware of cyber security issues associated with mobile phones.

Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?
Digital display only on web pages is the best option due to the possible extension of support period. Physical labelling makes it difficult to notify the customers the extension availability. In addition, physical labelling is problematic for a number of installed consumer appliances, such as air conditioners, hot water systems, pool pumps and home energy storage systems, where the consumer does not see the product on the shop floor. Digital labelling also gives the ability to provide more education on the label to consumers who are actually interested in security ratings across products.

Finally, implementation of proposed standards and labelling regulation (if decided) would be best managed by a proven, experienced regulator such as the ACMA. ACMA has the track record on wireless/internet regulation, the legislative powers and more importantly, the resources and experience in compliance and enforcement.

CESA and AREMA look forward to further consultation with the Department on the development of regulatory proposals and is happy to clarify any of the comments above.

Yours sincerely

[redacted]	[redacted]
Ian McAlister	Greg Picker
Chief Executive Officer	General Manager