AGL Energy Limited
T 02 9921 2999
F 02 9921 2552
agl.com.au
ABN: 74 115 061 375

Level 24, 200 George St
Sydney NSW 2000
Locked Bag 1837
St Leonards NSW 2065

Cyber, Digital and Technology Policy Division

Department of Home Affairs

Submitted electronically via Department of Home Affairs Submission Form

27 August 2021

Strengthening Australia Cyber Security Regulations Discussion Paper

AGL Energy Limited (AGL), appreciates the opportunity to provide comments on the Department of Home Affairs (the Department), Strengthening Australia's cyber security regulations and incentives discussion paper.

AGL is a leading essential services provider with a 184-year history of innovation in the provision gas, electricity, and telecommunications services to customers throughout Australia. AGL has been heavily involved in the creation of the Australian Energy Sector Cyber Security Framework (AESCSF), to ensure that the energy sector's security posture is uplifted and prepared for the increasingly complex cyber threat landscape.

In addition, AGL has been involved in the co-design process for the Security of Critical Infrastructure reforms including the amendment of the *Security of Critical Infrastructure Act* 2018 (Cth) and the associated sector specific rules and standards. The broadening of the scope of this legislation to now include eleven industries is considerable and wide-ranging. As a result, AGL will already be subject to cybersecurity standards and rules and does not consider additional frameworks would be necessary for the energy sector.

This excludes standards for smart devices as this is an area that AGL sees as lacking in basic standards and protections for both the security of the energy system and consumers. This is particularly important as our reliance on Internet of things (IoT) devices increases and simultaneously consumer levels of interaction with the devices increase. In establishing national consistent cyber security standards, it is important to protect the security of the device and the data associated with the device, as well as ensuring the standards do not inadvertently restrict consumers' ability to access relevant value streams through ownership and operation of the smart device.

Please find AGL's responses to some of the questions posed in the Attachment 1. AGL looks forward to working with the Department to ensure that any cybersecurity standards are fit for purpose and consider energy specific devices and customers. If you have any further questions about this submission please contact Marika Suszko, Wholesale Regulatory Manager at [redacted].

Yours sincerely,

Elizabeth Molyneux
General Manager, Policy and Markets Regulation

Attachment 1:

Question 8: Minimum standards for personal information
Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?
As mentioned above AGL has been heavily involved in the creation of the AESCSF framework and will also be captured under the Security of Critical Infrastructure framework for gas, electricity and telecommunications so will already be subject to cyber security standards. There are discussions occurring regarding the inclusion of Distributed Energy Resources into the AESCSF framework as well which would broaden its scope. AGL also notes that organisations similar to AGL are already subject to the notifiable data breaches regime and APP11 in the Privacy Act, which relates to the security of personal information. It is unclear how any proposed cyber security code would interact with the obligations under existing industry specific legislation and other proposed changes that are being considered for the Privacy Act. AGL does not consider additional standards would be required for sectors that are already subject to sector specific standards, as there is the potential for overlap, or potentially conflict, between the standards that AGL is already subject to, which would increase the regulatory compliance burden for organisations similar to AGL with minimal benefit to consumers. Given the pace at which technology is changing, a more practical way of promoting higher cyber standards may be to incorporate more practical guidance on cybersecurity into the OAIC's Guide to Securing Personal Information which is in the process of being updated.

Question 9: What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)? Again, AGL would direct the Department to the AESCSF framework.

Question 10: What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes? As mentioned above, industries that already have sector specific standards in place should be exempt from this code given the risk of duplication with existing standards.

Chapter 6: Standards for smart devices
Question 11: What is the best approach to strengthening the cyber security of smart devices in Australia? Why?
AGL would suggest Option 1 and implement mandatory standards for smart devices. As the Internet of Things continues to automate processes in many industries it is important to ensure there are basic protections for devices in the form of minimum standards. The ubiquity of IoT devices is likely not something which was foreseeable during the last review of the Privacy Act. Despite this, the technological neutrality of the Act provides users with appropriate privacy protections - particularly under APP 5 and APP 6. For example, organisations offering IoT devices are required to obtain appropriate consent and only use the information obtained for purposes permitted under the Act. This can be achieved by including appropriate terms in contractual agreements requiring the customer who is signing up for a particular IoT product or service to obtain consent from anyone who may have their data captured by the IoT device. In many cases, IoT devices which collect data from multiple individuals only collect aggregated data. Putting the onus on the contracting customer to obtain the necessary consents is preferable as there is administrative complexity with seeking multiple consents, particularly when the other members of the household are unknown and may change without notice. AGL believes that the technologically neutral nature of the Act allows for innovation whilst providing consumers with appropriate protection in this space.

In the energy sector electricity distribution businesses are seeking out Wi-Fi enabled solutions to control an increasing penetration of behind the meter Distribution Energy Resources (DER), including solar PV, home batteries, home management systems and Electric Vehicles (EVs). Distribution businesses are seeking ways to control these products to ensure system security and reliability. For example, in South Australia, the Government in 2020 introduced Smarter Homes regulations that give the distribution business and the Australian Energy Market Operator (AEMO) the opportunity to remotely control these products through the inverter or smart meter, in essence turning uncontrollable dumb devices into smart controllable generation systems. Distribution networks are also exploring the introduction of Dynamic Export Limits where solar PV will be actively controlled. This will mean the volume of DER based controlled generation will ramp up substantially in the next few years.

This is especially likely given the Energy Security Board's recommendations to the Federal and State Governments that other States follow the South Australian Smarter Homes proposal and seek out API based generation control for emergency back stop measures. AGL believes this is a rapidly growing cyber and system security issue in the energy sector, especially as the inverter manufacturing market is dominated by a small number of hardware vendors based overseas.

The Distribution Energy Integration Program (DEIP) Interoperability Steering Committee is currently prioritising, coordinating and steering the required activities to establish uniform interoperability and cyber standards to better enable DER integration. AGL welcomes Federal Government oversight and direction, given the significant role of State based distribution networks and the need for harmonisation of cyber security standards across these distribution networks. However, we encourage the Federal Government to leverage the work already undertaken and in progress by the DEIP group as part of establishing a national response.

Finally, while AGL supports nationally consistent cyber security standards for smart devices, we also caution that in developing these standards, consumers ability to maximise the benefits of their DER investment is not constrained. For example, if a consumer installs a home solar and battery system with smart inverter technology, the cyber security standards should not inhibit interoperability across hardware and software platforms and therefore inhibit consumer choice on the types of markets they want to participate in and be rewarded for offering up their DER for system and market services.

Question 12: Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices? Yes, this seems like an appropriate standard, but the list of applicable smart devices and appliances needs to be expanded to include digital meters and other energy related smart devices.

a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?

What does the Department consider the top 3 requirements, does that mean the first three listed in the standard? Clarification is required before this is answered.

Question 14: What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?

In order to provide a cost, estimate the breadth of the standard would need to be provided. For example, AGL would need to understand whether smart meters would be included in the standard.

Chapter 7: Labelling for smart devices

Question 16: What is the best approach to encouraging consumers to purchase secure smart devices? Why?

AGL suggests that ensuring that manufactures include automatic security updates for smart devices as this would mitigate some of the risk and ensure devices stay secure. Ensuring independent testing and providing a safety rating (similar to cars) would also ensure that devices are secure out of the box.

Question 17: Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

AGL believes a combination of standards for smart devices and labelling with expiry dates for smart devices would be the most effective approach to assist consumers with understanding the level of cybersecurity on their devices and when that protection is due to expire. This would only assist in the absence of auto-updates for devices which AGL suggests is a more effective measure.

Question 18: Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? a. If so, which existing labelling scheme should Australia seek to follow? AGL does not have experience in this area so cannot comment on the likely uptake of voluntary labelling schemes.

Question 19: Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not? Yes, as noted above this in combination with a basic cybersecurity standard for such devices would be a good start for an industry that is not very mature with regard to the security of its products.

Question 21: Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?
By providing a safety labelling mechanism this builds trust into the ecosystem also the recall process or immediate patching processes could be reuse for smart devices.

Chapter 8: Responsible disclosure policies
Question 22: Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered? AGL would like to see regulatory approaches to responsible disclosure considered as a preferred option.

Chapter 9: Health checks for small businesses
Question 23: Would a cyber security health check program improve Australia’s cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?
Smaller businesses are much less likely than large business to employ dedicated cyber security teams. If the Government was to provide small businesses with a low cost (or free of charge), “health check” service this has the potential to improve supply chain management for small businesses.