WATER SERVICES
ASSOCIATION OF AUSTRALIA

WSAA SUBMISSION

Strengthening Australia's Cyber Security Regulations and Incentives

27 August 2021

Cyber, Digital and Technology Policy Division

Department of Home Affairs

techpolicy@homeaffairs.gov.au

SUBMISSION: Strengthening Australia's Cyber Security Regulations and Incentives.

Adam Lovell	**Brendan Guiney**
Executive Director	Executive Officer
Water Services Association of Australia	NSW Water Directorate
Level 9, 420 George Street	
Sydney NSW 2000	
(02) 9221 0082	(04) 9876 5055
adam.lovell@wsaa.asn.au	brendan.guiney@waterdirectorate.asn.au

David Cameron	**Peter Morison**
CEO	CEO
Queensland Water Directorate	VicWater
43-49 Sandgate Road	2/466 Little Lonsdale Street
Albion QLD 4010	Melbourne VIC 3000
(07) 3632 6854	(03) 9639 8868
dcameron@qldwater.com.au	peter.morison@vicwater.gov.au

We confirm that this submission can be made available in the public domain.

Background

About WSAA

The Water Services Association of Australia (WSAA) is the peak body that supports the Australian urban water industry. Our members provide water and sewerage services to over 24 million customers in Australia and New Zealand and many of Australia's largest industrial and commercial enterprises. WSAA facilitates collaboration, knowledge sharing, networking and cooperation within the urban water industry. The collegiate approach of its members has led to industry wide advances to national water issues.

About NSW Water Directorate

The NSW Water Directorate is an incorporated association representing 89 local government owned water utilities in regional NSW, serving 1.85 million people. The NSW Water Directorate provides independent technical advice to local water utilities to ensure they deliver high quality water and sewerage services to regional communities in NSW. NSW Water Directorate works collaboratively with government and non-government organisations to support, advocate for and enable the needs of local water utilities in NSW.

About Queensland Water Directorate

The Queensland Water Directorate (qldwater) is a business unit of the Institute of Public Works Engineering Australasia Queensland. Their members include the majority of councils, other local and State government-owned water and sewerage service providers, and affiliates.

As the central advisory and advocacy body within Queensland's urban water industry, qldwater is a collaborative hub, working with its members to provide safe, secure and sustainable urban water services to Queensland communities. Major programs focus on regional alliances, data management and statutory reporting, industry skills, safe drinking water and environmental stewardship.

About VicWater

VicWater is the peak industry association for water corporations in Victoria. Their purpose is to assist members achieve extraordinary performance while helping to influence the future of the Victorian water industry. VicWater plays an important role in the Victorian water industry in influencing government policy, providing forums for industry discussions on priority issues, disseminating news and information on current issues to stakeholders, identifying training needs, and the production of performance reports and industry guides.

VicWater is focused on supporting Victorian water corporations and the broader industry in their objective to provide efficient and sustainable water and wastewater services in Victoria.

Introduction

WSAA welcomes the opportunity to provide the water sector views on strengthening Australia's cyber security regulations and incentives (the Paper). The water industry strongly supports the 2020 Cyber Security Strategy's focus and emphasis on the critical role cyber security has to play in the economy. Our detailed comments on the consultation paper are provided below.

Specific responses the questions posed in the consultation paper

Why should government take action?

1. What are the factors preventing the adoption of cyber security best practice in Australia?

Cyber security best practice is a constantly evolving area. Given the rate of change in cyber security occurring at present, trying to determine and adopt best practice in all areas of cyber security is unlikely to be possible. A better option would be to pursue good practice cyber security for key fundamentals.

The key fundamentals of good practice cyber security and factors affecting adoption are:

People: Security awareness level in water businesses has a direct impact on security implementation, especially at the management level. Having low level of security awareness can potentially cause delay or interruption to the adoption of cyber security good practice.

Process: Business processes should include consideration of cyber security implementation and application. This would be enhanced by education and the security awareness of personnel.

Technology: Legacy and modern technology must consider cyber security elements and how they impact people and process within the business in a manner that maximises the benefits of the technology whilst ensuring the relevant security controls and processes are in place to safeguard the technology from being exploited or used against the business.

2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

There is an increasing availability of low-cost options to exploit operating technology and information technology vulnerabilities. In addition, rapidly expanding technology choices have significantly increased the amount that consumers and small businesses need to be aware of to ensure effective cyber security protection. These factors mean the general consumer and small business often lack the time and capacity to understand all of the primary requirements needed for effective cyber security. Improving cyber security resilience for these groups requires clear and direct guidance for users along with certification of products.

Certification, along with associated regulations and standards should ensure technologies meet minimum-security levels to reduce business risk in the adoption of new technology. Such measures will significantly reduce the impact of negative externalities and information asymmetries on buyers of technology. Consumer education and clear certification labels will change manufacturer behaviour.

Government action is required to raise awareness about the standards that are expected of secure products, the certification and labelling schemes that available nationally and how consumers should interpret these. There is also a role for government in working with industry to clearly articulate good practice cyber security requirements and have these articulated into agreed codes of practice.

Current regulatory framework

3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?

The current regulatory framework has strengths in the areas of privacy protection. However, there are also significant gaps in relation to smart devices and the privacy of data collected by device and application owners. The default situation in Australia is that data is owned by the corporation providing the service, not the provider of the data. Reversing this ownership principle, with the emphasis on the data generator being required to provide permission for the use of the data would be a strong step to better protection of personal data on smart devices and apps.

Australian consumer law provides strong protections for the return of faulty or not fit for purpose goods. However, for smart devices and IoT devices additional rules are required to ensure protection of the consumer. Of particular importance is the need for the introduction of requirements for security by design principles in all digital products. Moving from the consumer being responsible for the security of all aspects of these devices to the manufacturer having an obligation to ensure appropriate in-built security for core device functionality in a way that is transparent to the user.

In addition, there are no rules governing the minimum device attributes required to effectively be able to maintain security of the device. The application of baseline requirements similar to the European Standard ESTI EN 3030645 V2.1.1 (2020-06) should be seen as a minimum level of protection for consumers and small businesses.

4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

The approach outlined in the consultation paper in relation to clarity, coverage and enforcement are supported as a critical first step. The application of baseline requirements similar to the European Standard ESTI EN 3030645 V2.1.1 (2020-06) would be of benefit in enhancing the ability to secure smart devices.

In terms of striking the balance, at present the balance is almost entirely on the consumer being fully informed, selecting all appropriate attributes of a product - yet these are not currently required to be made available to the consumer and then ensuring that the device is secured - even if the manufacturer has not provided sufficient embedded ability within the

device to achieve this. The current lack of key security information and options in relation to smart devices mean that relying on voluntary provision of the right information and services is an ineffective mechanism in relation to cyber security. A consistent national requirement for labelling and certification is required to enable these functions for all smart devices.

To make a significant shift in the current IoT security paradigm, a consumer-informed, market driven, industry-led certification and labelling scheme supported by Government is suggested, as outlined by the Internet of Things Alliance Australia (IoTAA). A certification and labelling scheme would provide consumers, business and governments with critical visibility and confidence of the independently verified security claims of the devices and solutions they are purchasing.

In addition, there is fundamental interplay between State and Federal regulators that needs to be resolved. Any new legislation needs to take into account current State and Territory regulatory arrangements to avoid regulatory duplication and unnecessary cost burden.

Governance standards for large businesses

5. What is the best approach to strengthening corporate governance of cyber security risk? Why?

Option 1 – Voluntary governance standard is preferred as the first step to start bringing business into the discussion and development of the standard. This will allow early adoption of the governance standard and ensure key benefits and areas for improvements are identified.

Mandating a corporate governance standard for cyber security is not a preferred approach. Any such move would need to consider the impacts on various existing regulatory and governance regimes in place at a State, Territory and jurisdictional level to avoid regulatory duplication and unnecessary cost burden.

6. What cyber security support, if any, should be provided to directors of small and medium companies?

Cyber security support ideally would promote best practice approaches and case studies in good practice cyber risk management for small and medium sized utilities – seeing is believing. Webinars and short courses would also be useful.

Security awareness exercises are critical to businesses to better understand the cyber security issues and how to manage them. They assist directors to understand the importance of cyber security preparedness and the effectiveness of their current business processes. Over the longer term it supports directors in understanding how well the business is adopting good cyber security practices.

7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

There would be benefit in the Australian Cyber Security Centre or the Joint Cyber Security Centre in each State or Territory offering basic training and awareness in cyber security. This could be augmented by video and other training aids. In addition, there would be value in a

national certification scheme for small and medium sized companies in relation to cyber security.

Note that a light handed, guidance-based approach would be preferred that focuses management's attention on consideration of the risks and costs from a cyber-attack relative to other common business risks. Such guidance should actively support leaders in how to incorporate these risks into their corporate risk registers and business continuity plans and ensure these documents are monitored and updated.

Minimum standards for personal information

8. 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?

A number of water businesses are covered by State or Territory based privacy requirements. Therefore, a cyber security code under the Privacy Act would not be the most effective option for the water sector. Rather the preference would be for a guideline or code of practice that provides a combination of principles-based components to achieve good practice along with specific minimum requirements in a manner that is flexible and cost-effective.

9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

The following technical controls would be considered key:

- Identity and Access Management: limiting access to personal data to authorised employees and third parties.
- Data Loss Prevention Tools: adding a layer of data protection.
- Encryption and Pseudonymization: Encryption protects against data theft. Pseudonymization will ensure data cannot be used to identify a subject (person) unless additional information is provided.

10. What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?

No comment.

Standards for smart devices

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

The water sector supports a consumer-informed, market driven, industry-led certification and labelling scheme supported by Government. A certification and labelling scheme would provide consumers, business and governments with critical visibility and confidence of the independently verified security claims of the devices and solutions they are purchasing.

The setting of a mandatory standard for smart devices can limit the flexibility of manufacturers and suppliers in implementation and can drive perverse market outcomes. Establishing a labelling scheme allows consumers the ability to choose the level of protection that they require for their particular application. A one size fits all solution isn't appropriate given the diversity of devices and their application, coupled with the rapidly changing security environment. Rather the consumer should be able to determine a cost appropriate product that meets their needs. This avoids undue cost and ensures fit for purpose protection.

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

Yes, but it is only one of a suite of available standards.

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

The standard should be used for reference purposes, as the basis for industry led certification process. The top three requirements are of high importance.

b) If not, what standard should be considered?

Whilst ESTI EN 303 645 has a number of advantages, it should be considered with other local and international standards including:

- Cyber Security for IoT: Baseline Requirements, which is similar to the UK (DCMS, October 2018) and in line with the Australian IoT Device Voluntary Code of Conduct (released by the Department of Home Affairs in September 2020).

Other standards bodies to observe in the IoT ‘smart’ device space are:

- ENISA with their publication of Baseline Security Recommendations for IoT, and
- NIST with their NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers.

Noting that higher level security claims should be based on recognised international security frameworks and standards.

13. [For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

Not applicable.

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?

No comment

15. 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?

No comment

Smart devices (Cyber CoP/Digital Strat and Arch CoP/SCADA CoP)

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

A simple rating system that is based on a core set of minimum cyber security standards for each different level, similar to the star rating system used in a number of certification schemes such as electrical and water devices. Such a system is already in use for other consumer products and is well understood. An approach consistent with the IoTAA Security Trust Mark is recommended to ensure that devices are appropriately validated and trusted by consumers, government and business. The labelling process must be clear to avoid confusion, easy to understand and well communicated by government.

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

A combination of labelling and voluntary accreditation should be pursued in a manner consistent with the IoTAA Security Trust Mark. The objective of labelling should be to provide sufficient clarity for consumers, government and businesses so that they are able to choose the product that best suits their needs, they can have trust that the products supplied meet the required level of security attainment. The scheme needs to have the flexibility to easily adjust to the rapidly changing smart device offerings and changes in the cyber security landscape. It must also require independent testing and validation of manufacturer claims.

(Option 1)

18. Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not?

No comment.

a. If so, which existing labelling scheme should Australia seek to follow?

No comment

(Option 2)

19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

This depends on the intent of the expiry date label. To be effective, a security expiry date would need be a product end of support date. Essentially a commitment from the manufacturer to provide security support to the product up to a certain date. It then helps

inform the consumer of the duration of any security support, and the need to upgrade or replace the product to ensure security is maintained.

20. Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

We are not advocating for mandatory labelling. However, we would support a comprehensive voluntary labelling scheme for mobile phones and other high use, high risk devices. A mandatory scheme would achieve a minimum level of security but is likely to act against timely security innovations and an effective ability to choose devices with different levels of security depending on need.

21. Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Physically will assist consumers in choosing a product. However, it is only likely to be valid for a given (short) time period.

Digital labelling – should always be provided to ensure informed consumer choice because of:

- Ease of access
- Allows customers to check the current security status of the equipment over time, particularly valuable when looking at second-hand equipment that is already in circulation.
- Allows a quick way to integrate continuous monitoring of security labels across many different products, which is useful for consumers and especially for businesses.
- Enables businesses to easily set up routine digital processes to automatically determine when to replace or update equipment.
- The information doesn't fade, disappear or get removed over time.

Responsible disclosure policies (for smart devices)

22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

The water sector would support voluntary approaches to increasing responsible disclosure. There would be value in the Government releasing guidance or toolkits to support industry in responsible disclosure. The introduction of mandatory requirements with responsible disclosure legislation with the potential for penalties for non-compliance are likely to be counterproductive, actively discouraging benign beneficial activity by agencies other than manufacturers. It is also likely to increase manufacturing overheads. This could be avoided or minimised through the use of a voluntary approach.

Health checks for small business

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?

Yes, a simple checklist or certification that was clear, low cost and easy to implement would benefit cyber security and improve the marketability of Australian products.

24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

As cyber security control requirements become more embedded in contracting requirements the ability to demonstrate attainment against a health check program is likely to improve the marketability of products.

25. Is there anything else we should consider in the design of a health check program?

No comment.

Protecting Consumers

26 What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

No comment.

27 Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

No comment.

Other Issues

29.What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?

No additional comment.