WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER INDUSTRY SUBMISSION

2023-2030 Australian Cyber Security Strategy

14 April 2023

SUBMISSION: 2023-2030 Australian Cyber Security Strategy

Adam Lovell	**Brendan Guiney**	**Linda Roberts**
Executive Director	Executive Officer	Interim CEO
Water Services Association of Australia	NSW Water Directorate	Queensland Water Directorate
Level 9, 420 George Street		Level 1, 9 Eagleview Place,
Sydney NSW 2000		Eagle Farm 4009
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Jo Lim	**Luke Sawtell**
CEO	Executive Chair
VicWater	Water Services Sector Group
2/466 Little Lonsdale Street	
Melbourne VIC 3000	
[redacted]	[redacted]
[redacted]	[redacted]

Submission key recommendations

The water sector supports the general intent of the Australian Cyber Security Strategy.

It should be noted that most larger water businesses are State or Territory owned entities, responsible to their State or Territory governments and subject to different State or Territory based regulatory regimes. However, there a number of water businesses that are Local Government owned, including some larger water businesses. It is important that Home Affairs recognises these diverse governance arrangements and does not seek to duplicate existing regulatory and support functions that exist in each State or Territory.

Detailed response to the discussion paper

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

- Australia wide testing and exercising of disconnecting from rest of world.
- Closer link with the checks of people who work in critical infrastructure or critical cyber roles, preventing malicious insiders.
- Centralised monitoring, alerting and management (SIEM services) for Australian based entities. So we can see real time what is happening and protect each other.
- Sharing of active threat information in real-time.
- Clear guidance on how we manage specific nation state entities as a country. Should we use their technologies and services? If so, are there any suggested restrictions on use, along with precautions or recommendations on how we might work with them to provide relevant services?
- Clarity on how training and education to uplift cyber maturity nationally.
- Alignment with international data protection and security frameworks such as the GDPR.
- Easily consumed standards for Board reporting on cyber security hygiene and maturity. This should allow comparison with like entities, benchmarking and assessment of maturity levels.
- Greater cooperation between the Commonwealth and State governments on cyber security with an emphasis on avoiding duplication and complimenting cyber security maturity improvement strategies, between both layers of government and industry sectors.
- A greater commitment from the Commonwealth to share relevant and timely cyber intelligence to industry and other stakeholders.

2. What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy?

- Better alignment between the State and Territory and Commonwealth legislation around Privacy, Health and security posture. Every state is slightly different and requires risk

assessment for data to be outside of most states (e.g. Health). Technology has shifted and data should be able to be held within Australia, the security posture is then the only differentiator.

- Be clear on approach to working with foreign entities, who we should and should not engage and what engagement can occur (e.g. data storage).
- One legislation to follow for all that is the baseline or minimum benchmark for entities to follow.
- One cyber reporting body for events to avoid overlap and confusion, not specific State and then Federal agencies.
- A clear Trustmark or similar scheme to verify the security of IoT and OT devices, similar to that proposed by the Internet of Things Alliance Australia. This would need to include a validation check on the hardware, firmware and software. The approach could also be extended to include Audio Visual, IT and other devices.
- The Office of Supply Chain Resilience in the Department of Industry, Science and Resources should better coordinate with industry and be prepared to share more timely supply chain intelligence.

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

- Utilise industry expert groups to define cyber maturity and controls relative to their industry or business sector and incentivise organisations to include these as critical risk controls in their business.
- Centralised Govt SIEM available to all, reduce duplication and cost.
- Pen test services run by a centralised government agency, which is not a regulator, such as the ACSC. This service would need to be provided at reasonable cost, with the acknowledgement that some things that are found will not be a risk and therefore require no action.
- If a legislative approach is to be implemented, consideration of a single piece of legislation on cyber that cascades and compliments existing or renewed legislation within states and jurisdictions. Consider the same approach for Privacy legislation.
- Cyber Support services for smaller entities.
- Real-time threat sharing information.
- Clarity on working with foreign entities, particularly the approach to take with entities based on risk.
- Clear security labelling requirements for devices to confirm their level of cybersecurity protection, and ensure devices are capable of having their security regularly updated. This should be accompanied with Hardware, firmware and software 'ticks' of verification.
- Minimum intrinsic cyber security requirements for all OT and IoT devices.
- Guidance for industry and consumers about recommended levels of cyber security protection for OT and IoT devices to support interpretation of security labelling requirements.

b. Is further reform to the Security of Critical Infrastructure Act required?

It is too early to determine at this point. This question should be revisited after the amended SOCI Act has been in place for a reasonable period or when the Commonwealth reveals its anticipated cyber security legislation.

It is likely that making amendments to the SOCI Act to direct further cyber uplift would require the implementation of additional legislative reforms to direct uplift in other industry and business sectors outside of critical infrastructure sectors,

b.i. Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The sector agrees the need for change. Our view is that most events that lead to a breach of a Critical Infrastructure Asset are likely to come from partners and their sub-contractors and partners / sub-contractors. These are not well captured under the Critical Infrastructure (CI) Act are not really thought of under the CI banner. For example a partner sub-contractor who provides equipment is breached, that breach penetrates the partner and then into the CI entity. This is a real risk for our connected society. However, in doing this the outcome and approach should be determined in consultation with those affected by the CI Act before making changes to the Act.

The cyber baseline should be across all organisations, as it is difficult to confirm the information and partner's systems that a sub-contractor to a delivery partner will have access to.

A concern in including customer data is the complexity caused by the interaction between the cyber security and Privacy Act. It is suggested that any additional requirements for customer data are called up under the Privacy Act.

Systems is a very broad term, covering anything from a digital architecture to a collection of Applications, to a software system. Extending the CI Act in such an undefined manner is not supported.

c. Should the obligations of company directors specifically address cyber security risks and consequences?

The current obligations on company directors include ensuring management of cyber security risks and consequences under the ASIC Rules. There is no need for additional regulatory obligations. Any additional specific obligations should be placed under the ASIC rules. Noting that an overreaction in this area could result in needless gold plating and embellishment. The key focus should be to ensure governing bodies are presented with the right information, at the right time.

Balance is needed. Directors should be liable for poor cyber management, but overreaction in what is a rapidly developing area may lead to judicial grey areas.

d. Should Australia consider a Cyber Security Act, and what should this include?

Any approach should consider how to ensure a consistent national cyber security posture and consistency in the way businesses respond to that posture. This needs to be done in a manner where each entity is best placed to understand and manage their risks but needs to include consideration of the national posture. All options should be considered to achieve this outcome, rather than moving directly to developing a Cyber Security Act.

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

There is a need to understand business costs prior to implementation of regulation, and monitor increases that occur over time due to regulation. Comparing costs for industries of a similar nature that are regulated in Australia vs costs for those industries in non-regulated markets. There is also a need to understand overlaps and synergies between existing regulatory frameworks, particularly the Security of Critical Infrastructure Act, the Privacy Act and Criminal Code.

Governments should appreciate that there is a point in the cyber security investment curve beyond which security, however necessary it may be, cannot be afforded. In such instances, particularly when considering the connection between effective cyber security and national security, the government may need to subsidise aspects of cyber security, particularly for CI.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

(a) victims of cybercrime; and/or

There is a need for clarity here. The current ambiguity leads to a clandestine approach to the subject. If governments strictly prohibited ransoms, then cyber criminals would understand that there is nothing to be gained from organised extortion in this jurisdiction. There may be rare cases where ransoms need to be paid, but that should be done strictly under the supervision of law enforcement agencies.

A prohibition on payments simplifies the position for Boards. It pushes towards improved management of data and systems to avoid and minimise the impacts from ransomware. It provides clarity on the position to be adopted, particularly because this is known in advance. However, it removes the flexibility to pay a ransom where the value in payment outweighs the potential reputational and customer impacts.

(b) insurers? If so, under what circumstances?

Prevention of payment by insurers then places all of the payment obligation on the organisation subject to the ransomware attack. If there is legislation making payment illegal, then it will be necessary for organisations to self-insure against ransomware. As this will be done at the individual organisational level the results will be an increase in cost to consumer, but with highly variable outcomes in terms of actual protection from ransomware.

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

Refer f (a) above.

g. Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

This has already been made quite clear under the ACSC Guidance.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

- Through strong engagement with relevant government agencies and NGO's working to share and promulgate information about cyber threat management in rapid, accurate and timely manner.
- Harmonisation of cyber security approaches and legislation within regions.
- Australia Wide Exercises on cyber threats.
- Work towards real-time event management and information sharing.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

No comment

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

No comment

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

No comment

7. What can government do to improve information sharing with industry on cyber threats?

Provide clear and timely advice through the ACSC and other channels. We need more transparency in real-time about events. These should not be named entities but would be good to know the events in the related industry that are occurring in real time to enable a posture of readiness.

Look to establish sector communication groups for the rapid dissemination of information, within hours of a threat being detected. Provide a better mechanism for rapid sharing of

threat intelligence between sectors, similar to the Trusted Information Sharing Network. However, in doing this it is necessary that the communication is not through regulatory channels. The channels for this communication must be separated from the current Department of Home Affairs regulation and managed by a different department to build strong trust without the fear of sector implications from the timely disclosure of information.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

It is critically important to share cyber security incidents but to do so it is necessary to protect the potential confidence damage to organisations that a cyber security event may create. The water sector supports an explicit obligation of confidentiality to improve information sharing.

9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

No. The current approach sensationalises cyber security incidents. What is missing is the provision of detailed and clear explanation for how primary cyber security incidents occurred and steps that should be taken to prevent similar incidents. There should then be a mechanism to capture preventative measures and incorporate them into national guidance such as the ASD Essential 8.

10. What best practice models are available for automated threat-blocking at scale?

High enforcement on application whitelisting solutions under ASD8 (ML3) should be implemented as a minimum.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Yes, Provide clear and consistent requirements in relation to data security obligations. The capacity and awareness of cyber-security and data issues is much lower in smaller regional utilities. There would be strong value in providing targeted awareness training and good practice guidelines for regional Australia.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

No Comment.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

There is a risk that by enforcing a single reporting portal that the federal government will be creating regulatory reporting duplication. It would be preferable for the federal government to create platform that collates the information form the various regulators around the country for Critical Infrastructure sectors. For individuals a single reporting portal may provide to be an effective tool.

14. What would an effective post-incident review and consequence management model with industry involve?

The post incident model for safety incidents has been effective and would be appropriate for cyber security incidents.

The key elements are:

- Reporting to regulator,
- Regulator publication of the events (note confidential requirements will be required)
- Lessons learnt debrief and industry advice

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Through active collaboration and knowledge sharing in a trusted and confidential manner. For the water sector the Security of Critical Infrastructure Act provides a strong regulatory approach, including direct government intervention. Internationally, a more effective approach has been shown to be government collaboration coupled with rapid sharing of intelligence on emerging threats.

The current system with the Department of Home Affairs as both regulator and supporter doesn't work. It creates a significant conflict of interest because there isn't a clear separation of powers. This works against building trust and open disclosure. Separation of the support and communications functions from the regulatory areas is strongly recommended to drive changes that would significantly benefit the Australian economy.

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

No comment.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Provision of clarity in regulation along with clear, timely and reliable information on changes to the cyber security threat landscape. Enable each organisation to develop and maintain their cyber security posture based on the available threat intelligence. Trust the current organisational governance, through Boards, shareholders and stakeholders provide sufficient guidance and incentive to effectively manage cyber threats. The Federal Government should avoid an interventionist approach to management of cyber security threats.

17. How should we approach future proofing for cyber security technologies out to 2030?

Understanding and communicating effectively across all sectors and to the general public in a trusted and timely manner changes to the threat landscape along with mitigation approaches and relevant technological opportunities.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

These are two separate questions. They shouldn't be intertwined. The government can better use procurement as a lever to improve the cyber security ecosystem through the use of a Trust Mark or similar to indicate the level of cyber security protection intrinsically built into devices. In addition, there would be value in this Trust Mark embodying the risks relating to country of origin and sovereign concerns.

In terms of a viable path to market for cyber security firms. There is currently a national shortage of cyber security personnel. This means that a viable path to market is considered unlikely to be a primary concern for cyber security firms.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

As mentioned, this should be addressed through a Trust Mark scheme similar to that proposed by the Internet of Things Alliance Australia. It should focus on the approach that all new technologies should embrace a secure by design approach.

20. How should government measure its impact in uplifting national cyber resilience?

Given the number, scale and scope of recent cyber security incidents a direct measure would be a change in these parameters on an annual basis. In addition, useful metrics would be the number and scale of ransomware attacks, and the number of Australian residents impacted by the public disclosure of data through cyber security breaches.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

- Providing transparency on the process being adopted by government to introduce changes.
- Avoiding direct government intervention in the implementation of cyber approaches.
- Measuring overall business support and public sentiment behind the government's proposed changes. This could be through a net promoter score which should be positive and increase over time.

BACKGROUND TO SUBMITTING ORGANISATIONS

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.

About Water Sector Services Group

The Water Services Sector Group (WSSG) is the water industry group that forms part of the Federal Governments Trusted Information Sharing Network (TISN). The WSSG comprises the Risk, Security and Resilience experts from across the Australian water industry, focused on the enhancing the resilience of the national water sector. The WSSG works with the Department of Home Affairs as the primary conduit between Government and the sector, to translate government security and resilience policy into contextualised outcomes and activities for the water sector. This work includes improving understanding and resilience of cross sector interdependencies with other Critical Infrastructure Sectors

The WSSG has been the coordination point for the water sectors response to the SOCI legislation since its inception and will continue to play a lead role in developing the standard and guidelines that will guide the water sector in its approach to operationalising the SOCI legislative requirements.