WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER SECTOR SUBMISSION

Cyber security legislative reforms consultation on subordinate legislation

14 February 2025

Water Sector Submission: Cyber security legislative reforms consultation on subordinate legislation

Adam Lovell	**Luke Sawtell**
Executive Director	Executive Chair
Water Services Association of Australia	Water Services Sector Group
Level 9, 420 George Street	
Sydney NSW 2000	
(02) 9221 0082	(07) 3855 6119
adam.lovell@wsaa.asn.au	luke.sawtell@urbanutilities.com.au

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

This submission is not representative of the Water Corporation position as a Western Australian State Government entity.

Water sector submission to the Australian Government on cyber security legislative reforms

The water sector values the opportunity to provide feedback to the Department of Home Affairs (the Department) on the subordinate legislation introduced to operationalise the *Cyber Security Legislative Reforms (2024)*. In providing this submission we note that sector has provided detailed responses as part of the consultation process on the reforms to the Department of Home Affairs:

- submission to the Department of Home Affairs: CISC Legislative Reforms Restricted Consultation, 13 September 2024
- submission to the Department of Home Affairs: 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper 1 March 2024
- submission to the Parliamentary Joint Committee on Intelligence and Security: Parliamentary Committee Submission: Cyber Security Legalisation Package 2024, 25 October 2024.

This submission should be considered with reference to these earlier documents.

While the water sector appreciates the opportunity to provide feedback on the proposed rules, we are concerned that the consultation process has been compromised by conducting the consultation during the summer holiday period, with a number of workshops and deep dive sessions scheduled only weeks and days before the consultation process ended.

Given the limited opportunity that has been provided to consider the impact of the proposed rules, we suggest that a formal review of the legislation and its associated subordinate regulations be undertaken 12-18 months after implementation.

About the Water Sector Association of Australia

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

About the Water Sector Services Group

The Water Services Sector Group (WSSG) is the water sector 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 sector, focused on enhancing the resilience of the national water sector. The WSSG works with the Department of Home Affairs as the primary conduit between the Australian 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 sector's response to the SOCI legislation since its inception and will continue to play a lead role in developing the advice; standards; and guidelines that will shape the water sector's approach to operationalising the SOCI legislative requirements.

Security of Critical Infrastructure (Critical infrastructure risk management program) Amendment (Data Storage Systems) Rules 2024

The significant expansion of scope requires a transition arrangement

The Water Sector continues to be concerned that the proposed provisions are a significant expansion of the scope of the Critical Infrastructure Risk Management Program (CIRMP) and may require consultation with a range of external parties (e.g., business service providers and other data users). Responsible Entities will need sufficient time to assess, consult, adapt and comply with the provision. The Water Sector is concerned that the regulatory impact statement understated the potential costs and complexity for business. Consequently, we strongly recommend that a 12-month transition arrangement be provided, to allow time to conduct risk assessments and to develop appropriate risk-based controls.

Additional guidance and explanatory documentation are needed

The Water Sector notes that the definition of what may constitute business critical data is very broad and the proposed rules do not provide adequate guidance on how a Responsible Entity is expected to identify and assess business critical data. We recommend that the Department work with industry to develop guidance materials to assist with the classification and assessment process.

The Water Sector also notes that the proposed rules have been drafted in a highly technical way, while this will facilitate inclusion into the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*; the rules have not been accompanied with explanatory documentation, and we strongly encourage the Department to produce this material before the provisions are implemented.

Cyber Security (Security Standards for Smart Devices) Rules 2024

Minimum-security standards should be extended to commercial-grade devices

The Water Sector supports the establishment of minimum-security standards for consumer-grade internet-of-things (IoT) devices. However, we continue to question limiting the provision to consume-grade devices only as there is no clear reason for not extending these standards to commercial-grade devices.

Given it is likely that the Australian Government will regulate to protect commercial-grade devices in the future, we reiterate our earlier feedback:

- Expanding the Secure by Design Standards to cover industrial control devices, as is done in Europe and the UK. With a prioritisation based on the perceived risk to economy.
- The water sector would prefer full adoption of the EU's policy position on Smart Devices.
- We support the formation of an IoT device register to ensure that a certificate of compliance is legitimate.
- In implementing secure by design requirements, whilst they won't be applied retrospectively, given the extent of IoT device implementation by the Water Sector, there is a need for a suitable transition time coupled with an option for financial assistance if a

compressed implementation timeframe is required. It is important that there is good engagement with all Critical Infrastructure sectors to ensure the requirements are economically justified. This is particularly important for the water sector as our pricing and cost-recovery arrangements are highly regulated, with few opportunities to amend our pricing outside of the typical 5-year regulatory cycle.

- The Standards should be written in a manner that allows a risk-based approach to mitigate the risk from installed devices, where the organisation can demonstrate sufficient cyber maturity to adequately manage the cyber security risk.

Ransomware reporting obligations

Ransomware reporting requirements should be streamlined, and codified in the rules

Although Section 27 (4)(b) of the *Cyber Security Act 2024*, states that a ransomware payment report must be given in the manner (if any) prescribed by the rules, the proposed rules do not include any details of how or to whom the report is to be made. As ransomware reporting is a regulatory obligation, the rules should provide clear guidance on the reporting arrangements.

The sector is concerned that there is no consistency with the cyber security incident reporting obligations that exist under the *Security of Critical Infrastructure Act 2018*. Given it is unlikely that a Critical Infrastructure Entity would lodge a ransomware report in isolation from a cyber security incident. It is Water Sector's recommendation that the reporting arrangements be streamlined, with all reporting to be provided to the Australian Signals Directorate, and for this to be codified in the rules.

Cyber Incident Review Board

Improvements will ensure industry participation on the Cyber Incident Review Board

The requirement to for all Board and Expert Panel members to hold an Australian Government (or equivalent) national security clearance granting access to at least secret level potentially limits industry participation on the Cyber Incident Review Board. While many water sector participants do hold appropriate clearances, all such clearances are sponsored by a State or Federal government agency, creating a potential perception of bias or conflict of interest. This can be addressed by incorporating into the rules a provision that clearances for suitably qualified appointees, including those without a current clearance, may be sponsored by the Department of Home Affairs.

The rules do not include an expectation that industry representatives will be appointed to either the Board or Expert panel. If a cyber security incident involves or impacts a critical Infrastructure entity, the rules should impose an obligation on the Minister (for Board appointments) and the Chair (for Expert Panel appointments) to consider appointing a representative from the impacted industry sector to each review. In addition, if an incident impacts a State/Territory owned critical infrastructure entity, then a representative from that jurisdiction's government should be appointed to that review.

Telecommunications Sector Security Reforms (TSSR)

Although the TSR reforms appropriately address the issue of regulatory divergence between the telecommunications sector and the wider critical infrastructure community, the arrangements do not adequately address the issue divergent risk, regulatory and compliance arrangement that may result from co-location of telecommunications assets on located on other entities' owned land or physically attached to another regulated entities' infrastructure.

The Water Sector has raised these issues with the Department in the past, noting that the telecommunication sector had been given a right of access under its previous legislation and recommends that the revised rules include a provision obliging critical entities to formally consult regarding co-located assets.

As part of this consultation process, the risk management arrangements of the land and/or asset owner must be prioritised over those of the hosted asset owner, who if implementing different arrangements must be obligated to ensure they provide a level of risk mitigation that is at least commensurate with that of the primary asset owner.