WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER INDUSTRY SUBMISSION

2023-2030 Australian Cyber Security Strategy:
Legislative Reforms Consultation Paper

28 February 2024

SUBMISSION:

2023-2030 Australian Cyber Security Strategy:

Legislative Reforms Consultation Paper

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	
[redacted]	[redacted]
[redacted]	[redacted]

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

BACKGROUND

About Water Services Association of Australia (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 on national water issues.

About Water Services Sector Group

The Water Services Sector Group (WSSG) is the water industry group that forms part of the Federal Government's Trusted Information Sharing Network (TISN). The WSSG comprises the risk, security and resilience experts from across the Australian water industry, focused on 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 Sector Groups.

The WSSG has been the coordination point for the water sector's response to the *Security of Critical Infrastructure Act 2018* (the SOCI Act) 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.

EXECUTIVE SUMMARY

The table below provides a high level summary of the water sector's response to the Measures outlined in the *2023-2030 Australian Cyber Security Strategy: Legislative Reforms - Consultation Paper*. The submission contains detailed industry responses to the Measures, and the table below is to be considered indicative in nature.

Measure	Water Sector Response
Measure 1: Secure-by-design standards for IoT devices	**Supports** Security-by-design standards applied to IoT devices should apply equally to consumer and industrial devices. Consideration required of timeframes for suppliers and end users to implement.
Measure 2: Ransomware reporting for business	**Does not support** Contrary to the industry-government partnership arrangements that has been developed through the ACSC's mutual trust and confidence building measures. Significant burden in duplication of reporting. Prefer creation of a voluntary no-blame/just culture reporting methodology to encourage voluntary reporting of cyber-extortion events.
Measure 3: Encouraging engagement during cyber incidents	**Supports in principle** Supports the creation of the proposed limited use arrangements as an appropriate measure to encourage industry to cooperate with Government following a cyber-security incident. The limited use provisions must be supported by a no blame/just culture framework to provide the sector with confidence that punitive regulatory action would only be contemplated if a responsible entity was demonstrably engaged in wilful, deceptive or fraudulent behaviour.
Measure 4: Cyber Incident Review Board	**Supports** The CIRB needs to be separate to the regulatory enforcement arm of government for cyber security. Any information voluntarily provided must be protected from public release, including release by Government agencies under Freedom of Information (FOI) provisions. Data provided to the CIRB should be provided protection from being obtained via legal class action requests. Information, if to be disclosed, should not include any information that may expose an organisation to further targeted attacks.

Measure	Water Sector Response
Measure 5: Data Storage systems and business critical data	**Supports in principle** The proposed definition of business-critical data is too broad in application and may compromise or complicate the business' capability to use this information operationally and share information with third parties. There is a need to tighten the definition of business-critical to only include data related to CI Assets and their operation.
Measure 6: Consequence management powers	**Partially supports** Respect required for State jurisdictional powers. Water entities cannot be given a direction, if the entity advises in good faith that it cannot comply with the direction (for health, safety or operational reasons), or if it conflicts with another ministerial (Federal or State) direction. When providing a direction, by taking this action the Federal government has explicitly assumed responsibility for command, control and coordination of an incident.
Measure 7: Protected information provisions	**Supports** Protected information provisions be amended to clearly state that responsible entities are free to use protected information within the entity and the responsible entity can freely share this information with third parties for operational, regulatory and contractual purposes. Recommends that the Secretary be obliged to consult with the responsible entity and jurisdictional owners and regulators, and have regard for any advice provided by the entity, before releasing the information.
Measure 8: Enforcing critical infrastructure risk management obligations	**Does not support** The power to direct an entity to amend a deficient CIRMP must reside with the Minister, not at officer level. Focus must be on compliance with the SOCI Act, and not dictate risk appetite or controls within a CIRMP. Creation of a possible penalty clause for non-compliance further undermines the Department's commitment to collaborative rather than coercive approach to strengthening critical infrastructure security.
Measure 9: Consolidating telecommunications security requirements under the SOCI Act	**Supports** Consolidation provides an opportunity to strengthen CI security inter-dependencies by incorporating into the CIRMP arrangements an obligation on responsible entities to ensure their operations and risk management arrangements do not compromise the security, integrity or operations of another regulated entity.

SUBMISSION

Introduction

The water sector values the opportunity for consultation in relation to the *2023-2030 Australian Cyber Security Strategy: Legislative Reforms - Consultation Paper.* The sector welcomes and appreciates the Government's commitment to engagement on regulatory and non-regulatory measures to strengthen critical infrastructure (CI) security.

The water sector is committed to maintaining our trusted and collaborative partnership with the Department of Home Affairs in the management of all hazards risks because we share the Government's concerns about a rapidly evolving external security environment. While we acknowledge the dynamic nature of the evolving security environment, we are concerned that the Government is continuing to develop new regulatory measures without providing an appropriate level of support, or the opportunity for earlier CI security reforms to develop and mature. The industry notes that regulatory measures is only one of a range of measures which can effectively and efficiently, minimise and mitigate the complex and dynamic security threat landscape. We also note that by seeking to continually refine CI security legislative arrangements the Government diverts industry effort and attention away from managing security risks towards compliance with new regulatory initiatives.

The water sector represents a highly distributed nationwide infrastructure that reflects not only the range of State and territorial diversity in context, but a diverse range of ownership models predominantly State and or municipally owned, and monopolised. This can present a range of hard conflicts between individual contexts, freedoms and limitations, and the intent and objectives of Federal Government in addressing the national security risks.

Responses to Part 1: New cyber security legislation

Measure 1: Secure-by-design standards for IoT devices

The water sector fully supports the policy objective of implementing secure-by-design standards into the Internet of Things (IoT). However, the focus on consumer-grade IoT without a commensurate secure-by-design standard for industrial devices, risks creating a parallel market of less-secure and/or differentiated regulated market for industrial devices including devices integrated into the water-sectors' industrial control systems. The water sector recommends that secure-by-design standards should apply to technology commonly used across water and other infrastructure sectors, including CCTV/surveillance systems, access control equipment as part of security systems, and drones (unmanned aerial vehicles (UAV) and remotely piloted aircraft (RPA)).

The current device risk profiling from the US and Europe for IoT devices indicates a high potential for many industrial control systems to have potential security compromise risks. These countries are looking to mandate secure by design principles for industrial IoT devices to minimise the risk of compromise, particularly by state actors.

Should the Government's risk appetite regarding these devices change in the future, industry will be faced with high-costs to modify or remove these devices. The costs associated with

the Government's decision to remove of Chinese manufactured Closed Circuit Television (CCTV) and intercom systems from Government facilities in 2023, is illustrative of the potential consequences of a future change in risk appetite. For the water sector this is even more problematic as the sector works in cost-controlled and consumer-price regulated markets, which limits the sector's capacity to recover unplanned capital costs outside of limited regulatory pricing windows. For this reason, the sector believes that any security-by-design standards applied to IoT devices should apply equally to consumer and industrial devices.

The sector is supportive of ETSI EN 303 645 as a secure-by-design standard for IoT devices rather than defining a local specific standard, considered as an alternative in the proposal.

Creating an exclusion list of smart-devices is not recommended, as it has the potential of creating parallel markets for smart-devices that will only create confusion on the market and make any potential change to exclusion list in the future much more difficult to manage from a transitional measures standpoint.

Timeline to transition to the new standards for IoT devices should differentiate between suppliers to comply within 12 months while consumers should be allowed a longer timeline that accounts for business planning and lifecycle management of assets. On time-frames for adoption of any mandatory secure-by-design standards for IoT, the sector is highly constrained by pricing regulations. The majority of water industry participants operate under a five-year pricing cycle. While the costs for a secure-by-design device may fall in the medium-term, the small number of available devices and Australia's small market suggests that compliant devices will be impacted by significant cost rises in the short-term. For this reason, the sector suggests a 12 month transition period for suppliers of IoT devices and should the water sector be obliged to remove non-compliant devices, a further three-to-five year transition period is appropriate.

It is noted that the Government has indicated a preference to follow the UK Government's policy to exclude smart meters from the legislation. In the UK the rationale for this exclusion was the belief that these devices have sufficient protections under existing legislation. The Australian water sector submits that the current legislation regarding smart meters, particularly IoT devices is not adequate. For example, there are no legislative requirements for smart meters to have the option for software upgrades, nor the ability to enable software upgrades and security patching. Whilst the cyber security exposure can be limited by only installing devices capable of one-way communication, there is a growing functionality in smart meters which is primarily enabled by two way smart meter communication. Such communication requires the ability to assess the device against secure by design principles. The sector would support smart meters being included under the secure by design legislation.

Measure 2: Ransomware reporting for business

As demonstrated during the national cyber exercise AquaEx 2022, the resilience of the water-sector has historically contributed to a comparatively low level of ransomware and cyber-extortion vulnerability.

Discussions within the sector indicated that most water-sector participants will not pay ransoms, although a payment decision may be subject to the provisions of any cyber-security insurance policies they may carry. Should an industry participant, in particular those participants that are responsible entities under the SOCI Act, be subject to an actual or

potential ransomware attack, the participant would voluntarily report the incident to the Australian Cyber Security Centre (ACSC), regardless of any regulatory obligation to do so. Participants are also likely to have mandatory reporting to their state or territory owners and/or regulators. The proposal should consider the reporting mechanism(s) already in place and introduce the capability to aggregate this reporting at national level, without creating additional burden and obligation to the participants. Focus needs to be on the simplification and consolidation of reporting obligations – reporting to too many agencies during a cyber incident can be significantly time consuming and may result in a focus on reporting over remediation.

This suggests that implementation of a Federal mandatory reporting regime is unnecessary for the water sector, particularly given the government ownership of larger water supply entities, and may just be regulatory duplication. A mandatory reporting regime would also be contrary to the industry-government partnership arrangements that has been developed through the ACSC's mutual trust and confidence building measures including disclosure of information for specific purposes, and would have the unintended consequence of focusing industry on regulatory compliance rather than voluntary reporting, and benefitting from practical Federal assistance.

If such reporting is required, then there needs to be clarity about what events are reported. There is a need to clearly define what a reportable attack is. It will create a significant regulatory burden if all potential and failed attacks are reported. Ideally reporting would only be for a successful attack, or an attack that has had an impact on business operations.

The introduction of this reporting should not be associated with a penalty for non-compliance, or possibly even prosecution for ransom payment. Instead it should be treated in similar way as the other cyber incident reporting activity, where the information is shared for awareness at state and national level. Follow-up and support to resolution, or post-incident analysis should be similar to the other types of cyber incidents.

From the water-sector's perspective a better strategy for increasing the government's understanding of ransomware and cyber-extortion would be through creation of a voluntary no-blame/just culture reporting methodology to encourage voluntary reporting of cyber-extortion events to the ACSC. Shifting from mandatory to voluntary reporting obligation will also remove the need to establish a threshold that defines which entities are required to report. The reporting could be made obligatory for those entities falling under SOCI Act.

On reporting cyber-extortion lessons to industry, anonymised reporting has some awareness value, and generalised information does assist industry to develop and implement response arrangements. However detailed sector-level briefings with a greater level of tactical and operational detail are significantly more effective strategically for strengthening sectoral resilience. To this end, the sector supports the use of targeted and detailed sector specific briefings with key staff that have appropriate security clearances. Generalised briefings that summarise publicly available information are of very limited value.

Measure 3: Encouraging engagement during cyber incidents

Prior to the development of the SOCI Act, a number of water-sector entities (primarily those now designated as responsible entities) had developed close working relationships with the Australian Signals Directorate (ASD) and ACSC, based on a shared commitment to CI security objectives. Underpinning this relationship was the non-regulatory structure of the arrangements and confidence in ASD/ACSC assurances of confidentiality.

The passage of the SOCI Act, which included mandatory reporting obligations, step-in-powers, enforcement provisions and arrangements allowing agencies to share responsible entities' information with other government agencies, undermined the sector's confidence in the partnership arrangements. While the Cyber and Infrastructure Security Centre (CISC) has taken a number of confidence-building measures to restore trust, the CISC is a regulator with enforcement functions. Consequently, this changed the nature of the relationship with the regulated entities. The creation of a safe-harbour or limited use provision for the sharing of cyber-incident information and cyber-response actions would help rebuild industry's willingness to cooperate and share information with government agencies, as indeed would the incentive of a greater clarity and understanding of how the Government would assist the entity during the cyber incident.

However, the sector views that the introduction of a functional limited use provision is impossible to achieve under the current regulatory arrangements, as it would appear to conflict directly with the *Intelligence Service Regulations 2020*, which state – '*These Regulations are intended to enable ASD under paragraph 7(1)(f) of the Act to cooperate with and assist the Home Affairs Department in the exercise of powers and performance of functions under the SOCI Act*'. This creates a significant conflict between providing support and regulatory enforcement. A more effective approach would be to separate the entity responsible for legislative enforcement from the organisation responsible for promoting information sharing and assisting with threat mitigation.

Nevertheless, the sector supports in principle the creation of the proposed limited use arrangements as an appropriate measure to encourage industry to cooperate with Government following a cyber-security incident. However, as a limited use provision provides less assurance than a 'safe harbour' the sector recommends that the limited use provisions be supported by a no blame/just culture framework to provide the sector with confidence that punitive regulatory action would only be contemplated if a responsible entity was demonstrably engaged in wilful, deceptive or fraudulent behaviour. The Government also needs to establish clear and distinct separation of the engagement and assistance functions and those of the regulator enforcement function. Establishment of a no blame/just culture framework would then also assist with the implementation of Measure 4.

Measure 4: Cyber Incident Review Board

As noted above, the water sector supports the establishment of a no-blame/just culture framework for responding to cyber-security incidents and by extension the establishment of a Cyber Incident Review Board (CIRB) to identify lessons that will enhance post-incident cyber resilience. The CIRB needs to be separate to the regulatory enforcement arm of government for cyber security.

On granting the CIRB powers to seek post-incident information, the sector's position is that the CIRB's information gathering powers should be voluntary, and time constrained to within 6 months of an incident occurring. Providing information in relation to an incident may be extremely time consuming, depending on the nature of the incident, and there should be a reasonable allowance for suppling information requested by the CIRB. There should be a clear delineation that the information to be provided is only for the entity concerned, not downstream or upstream entities.

However, an entities' voluntary cooperation with a CIRB investigation would provide a gateway for accessing the limited use provisions outlined in Measure 3. In addition, any

information voluntarily provided must be protected from public release, including release by Government agencies under Freedom of Information (FOI) provisions. Separately, data provided to the CIRB should be provided protection from being obtained via legal class action requests.

In other aspects of incident and emergency management the Government has developed significant momentum in the use of a Lessons Management process (e.g. as issued by the Australian Institute for Disaster Resilience) as means of sharing lessons, and broadly lifting Australia's capabilities. This has been demonstrated to have wide applicability and use across all three levels of government, NGO, CI, and communities. The function and approach of the CIRB should model and exemplify the Lessons Management process independent of any level of government, free to identify and recommend lessons to Government as well as non-government, while providing the Cyber Lessons process with the deep expertise of Government experts. A highly effective CIRB will lift Government and non-government entities equally, and by doing so encourage confident engagement.

Demonstrated independence will be a critical factor in building confidence in the CIRB and its investigations. As cyber-security events are likely to increase as Australia transitions into a digital economy, the CIRB should be a permanently established statutory organisation with an ongoing budget allocation, fixed term executive appointment and demonstrable independence from executive government. As well as being granted powers to investigate incidents and recommend cyber-resilience measures, a permanent CIRB should also have a policy and legislative recommendation mandate, to ensure alignment between legislative and non-legislative resilience measures and associated standards.

The CIRB should be empowered to independently conduct a review following a cyber-security event on the basis of its own mandates to understand and identify the threats and lessons of value to Australia.

It should be empowered and funded to independently conduct a review where requested by an entity impacted by a cyber incident for the benefit of the affected entity as well as identification of general lessons for all. In addition, it should be able to commence a review in response to a recommendation from the National Security Committee of Cabinet, Attorney General, Minister for Defence, Minister for Home Affairs, the Cyber-Security Coordinator, and applicable State government entities and departments.

The CIRB should report directly to Ministers and officials with national security responsibilities (primarily members of the National Security Committee of Cabinet) and should report regularly to parliament, most appropriately through the Parliamentary Joint Committee on Intelligence and Security. Reporting to the committee should not be limited to post-incident reviews but must include recommendations to adapt regulatory and legislative setting in response to changes in the cyber-security environment.

Information, if to be disclosed, should not include any information that may expose an organisation to further targeted attacks - e.g. incident response approach and procedures, technology stack, or control effectiveness.

Responses to Part 2: Amendments to the SOCI Act

Measure 5: Data Storage systems and business critical data

The water sector strongly supports the policy objective of appropriately protecting information and data storage systems. However, the sector is concerned that the proposed definition of business-critical data is too broad in application and may compromise or complicate the business' capability to use this information operationally and share information with third parties for example during projects or contract negotiations. There is a high risk that this could be interpreted to broadly and as such result in significant expense for organisations to risk management and remediate risk. This risk is significant for many organisations and in many instances may be cost prohibitive to fully address.

The sector points to the complexity and confusion created by the SOCI Act's definition of protected information, the offence provisions (Section 45) and the poorly drafted information sharing provisions (Sections 41-44). The creation of a new class of business-critical data, with data protection and reporting obligations, is highly likely to create similar confusion and complexity. The sector recommends that the protected information provisions be amended to clearly state that responsible entities are free to use protected information within the entity and the responsible entity is free to share this information with third parties for operational, regulatory and contractual purposes (this would align with the policy intent of Measure 7).

The broad nature of the definition for business-critical data also has the potential to extend into customer data and other data covered by the Privacy Act. This has the potential to broaden the SOCI Act requirements to cover the entirety of a water business's operations. It also creates potential conflicts between different federal legislation. There is a need to tighten the definition of business-critical to only include data related to CI Assets and their operation.

The sector supports the proposal to incorporate data and information protection measures into the responsible entities' critical infrastructure risk management program, provided the development and implementation of risk management controls remains fully within the remit of the entity. Consequently, the sector sees little value in creation of an obligation to provide operational, ownership and control information to the Cyber and Critical Infrastructure Security Centre.

The proposed compliance threshold for management of data protection on systems holding personal information of at least 20,000 individuals is appropriate but must be accompanied by clearer advice regarding how-long organisations are obliged to hold individually identifiable information. For example, Australian Tax Office obligation to hold financial information for seven years, significantly increases an organisation's holdings of personal and sensitive information.

Measure 6: Consequence management powers

The water sector partially supports the expansion of consequences management powers, with the following recommendations:

- During the consultation with the affected entity the Minister must give consideration to any feedback provided by the entity on the potential consequences of the direction.

- The local state or territory authority overarching the sector for respective entity should be included in the chain of decision-making process, or consultation.
- The entity cannot be given a direction, if the entity advises in good faith that it cannot comply with the direction (particularly for public health, safety, environmental, regulatory or operational reasons), or if it conflicts with another ministerial (Federal or State) direction.
- Once a direction is issued, it must be clear that by taking this action the Federal Government has explicitly assumed responsibility for command, control and coordination of the incident and its consequences.
- In complying with the direction, the responsible entity must be indemnified from criminal as well as civil liability.

When using the consequence management powers, the Minister must respect jurisdictional arrangements and understand that the water sector entities are regulated under jurisdictional arrangements and the majority are government owned organisations. The Minister, in exercising consequence management powers is accountable to jurisdictional owners and regulators for the directions and consequences.

Measure 7: Protected information provisions

As noted in the sector's response to Measure 5, the sector supports amendments to the protected information provisions of the SOCI Act.

The sector recommends that protected information provisions be amended to clearly state that responsible entities are free to use protected information within the entity and the responsible entity can freely share this information with third parties for operational, regulatory and contractual purposes.

In relation to the Secretary's powers to release protected information, there is a risk that release of information without contextualisation may create additional harm or risks. The sector recommends that the Secretary be obliged to consult with the responsible entity and jurisdictional owners and regulators, and have regard for any advice provided by the entity, before releasing the information. This obligation would not be invoked if the information was released for law enforcement or intelligence purposes or if it was impractical to consult due to issues of timeliness or operational necessity.

The issue is further compounded by confusion of SOCI Act 'protected information' with the definition of 'PROTECTED' information as contained in the Federal Protective Security Policy Framework (and various other State frameworks). This requires clarity and resolution.

Measure 8: Enforcing critical infrastructure risk management obligations

Throughout the development of the SOCI Act, the Department of Home Affairs and the CISC has consistently emphasised that it is industry is best-placed to understand organisational risk and responsibility for developing organisation-specific controls. This measure demonstrably undermines this commitment.

By empowering the Secretary with a direction power, a power that is presumably delegable, those at officer level will be empowered to intervene in the day-to-day management of a responsible entity. It must be understood that for the water sector, risk management is not an occasional or periodic issue but an ongoing behaviour that underpins public confidence,

public safety, operations, asset management and investment decisions. By creating a power to direct an entity, without an appropriate contextualised understanding of the potential adverse consequences of compliance, the Government is likely to create a range of material risks. It is the sector's position that under Australia's system of government this power should only be rarely exercised by a Minister with due consultation, not an official.

The proposed obligation ignores the fact that the majority of water sector responsible entities are owned by, regulated by, and answerable to state, territory or local governments.

For these reasons, the sector does not support the Measure. Nevertheless, the water sector accepts that changes in the security environment may require changes to an entities CIRMP and recommends the following:

- The power to direct an entity to amend a deficient CIRMP must reside with the Minister.
- Before issuing a direction the Minister must consult with the entity and the relevant jurisdiction government before issuing a direction.
- During the consultation with the affected entity the Minister must give full consideration to any feedback provided by the entity on the potential consequences of the direction.
- Should a Direction be issued to an entity, then the federal government will take full responsibility and accept all liability associated with the required action. This includes all known and advised potential consequences associated with a directed action. For example, a Direction to a water utility could cause adverse public health outcomes, or damage to property, environment or reputation or loss of life. If the Direction is issued contrary to expert advice then the consequential liability and damages arising should accrue to the federal government.
- The financial implications of a given direction be transparent to jurisdictions' price setting structures and allowed for in cost-recovery directly or indirectly.

Creation of a penalty clause for non-compliance further undermines the Department's commitment to collaborative rather than coercive approach to strengthening critical infrastructure security. Given that the Department would only be able to review an entity's CRIMP by exercising the Act's information gathering powers, it suggests that CISC is planning to implement an audit and compliance program. There has been no consultation with industry on how such a program would work, what its governance structure may be or under what circumstances a review of a CIRMP would be initiated. Having invested significant reputation capital building industry's confidence in the CISC's regulatory philosophy the proposal of this amendment, without appropriate contextualisation, risks undermining the sector's trust in the CI security arrangements.

In addition, the proposed legislative change does not appear to recognise the current long standing State /Territory emergency management arrangements, which must always have primacy in jurisdictional cyber related 'hazard/emergency' events.

Measure 9: Consolidating telecommunications security requirements under the SOCI Act

The water sector supports consolidation of telecommunications security requirements under the SOCI Act.

A specific issue for the water sector has been the right of access arrangements granted to telecommunications providers. While the sector supports the telecommunications sector's

access to water sector assets for the purposes of installing or maintaining their equipment, exercise of this right must not compromise the security of the water sector's assets. For example, telecommunication providers should not damage, remove or compromise another entities' physical security controls when accessing their asset.

The water sector position is that consolidation provides an opportunity to strengthen CI security inter-dependencies by incorporating into the CIRMP arrangements an obligation on responsible entities to ensure their operations and risk management arrangements do not compromise the security, integrity or operations of another regulated entity.

CONCLUSION

The water sector appreciates the opportunity to comment on the *2023-2030 Australian Cyber Security Strategy: Legislative Reforms - Consultation* Paper, and is committed to working with the Government to develop and implement regulatory and non-regulatory measures to strengthen critical infrastructure security.

Whilst our detailed responses to the proposed Measures are outlined earlier, in closing we wish to remind the Government of the following water sector specific issues which can impact upon the sector's ability to deliver these Measures:

- The water sector operates in a highly cost and revenue regulated environment, typically on a three to five year budget lifecycle. This results in significant challenges to both sourcing funding and the timeframes for implementation of legislative changes at the entity level – this needs to be considered when setting regulatory obligations.
- The sector operates largely under ownership of, and regulation by, the States. This environment already brings with it a range of statutory risk management obligations, incident reporting and assurance measures. There is a significant risk of regulatory duplication between the States and Federal Governments with some of the Measures suggested, and we seek to see this minimised as far as possible. Steps to see this already available data aggregated, rather than introduce additional reporting, are required.
- The sector has always aimed to work collaboratively with Federal organisations (ACSC, ASD, CISC), and on an open voluntary basis. This in our view has fostered good relationships and exchange of information on risks to critical infrastructure. There is a danger that the introduction of an excessive number of mandatory regimes, potentially with financial or criminal penalties, erodes this current position of trust, with organisations reluctant to share information in future for fear of prosecution.

Finally, the sector remains concerned that the Government has moved to further implement legislative change without providing opportunity for industry to demonstrate that we have delivered an actual uplift in critical infrastructure security. The positive security obligations of the SOCI Act have been in place for less than 12 months, and consequently, there has been no analysis of the success of the obligations and any assessment of gaps and areas for refinement, before moving to a legislative response. If this process continues, industry is forced to constantly review compliance obligations, rather than focus on the delivery of true critical infrastructure security for the nation.

We trust you find this submission of benefit in your deliberations.