WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER INDUSTRY SUBMISSION

Proposed amendments to the Security of Critical Infrastructure Act 2018 (Cth): Draft Impact Analysis

22 March 2024

Amendments to the Security of Critical Infrastructure Act 2018 (Cth): Draft Impact Analysis

Adam Lovell
Executive Director
Water Services Association of Australia
Level 6, 75 Elizabeth Street
Sydney NSW 2000

(02) 9221 0082
adam.lovell@wsaa.asn.au

Luke Sawtell
Executive Chair
Water Services Sector Group

(07) 3855 6119
luke.sawtell@urbanutilities.com.au

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

Background

About WSAA

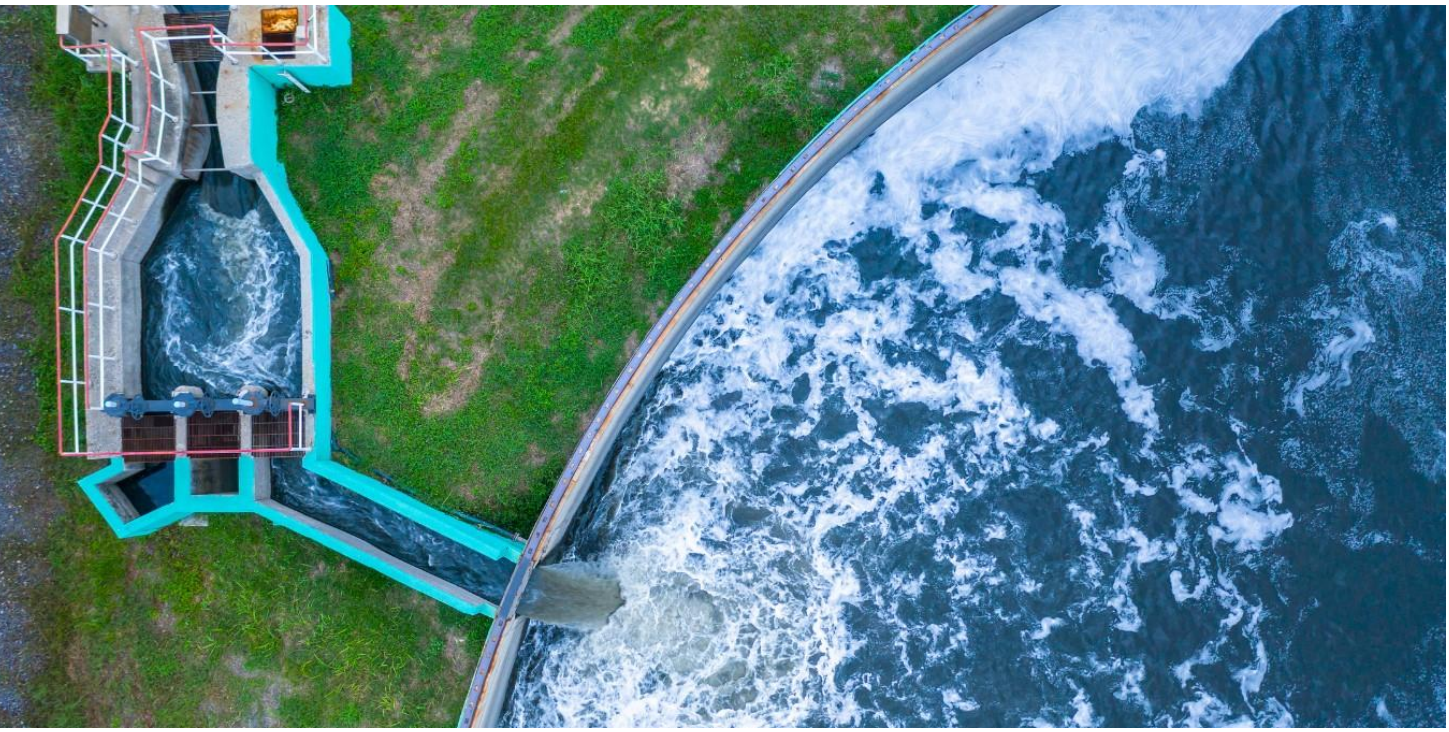
The Water Services Association of Australia (WSAA) is the peak body that supports the Australian urban water industry. Our members provide water and sewerage services to over 24 million customers in Australia and New Zealand and many of Australia's largest industrial and commercial enterprises. WSAA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



1. Introduction

The water sector shares the Commonwealth Government's concerns about a rapidly evolving external security environment and values the opportunity to provide comment on the regulatory impact of the proposed amendments to the Security of Critical Infrastructure Act 2018 (Cth).

Concerns

However, the water sector remains concerned that Government continues to develop new regulatory measures without allowing existing measures to mature, and without appropriate consideration of non-regulatory measures.

While the draft impact analysis claims that a preferred option has not been selected, this claim is disingenuous. It is clear that the federal Government is championing legislative change. Indeed, these changes have been proposed before the first compliance attestation has been submitted and before the previously introduced grace period for the last tranche of cyber-security measures has expired.

Consequently, it is difficult to take at face value the Government's claim that proposals for implementation of further regulatory measures are just one option under consideration. It is the water sector's position that moves to introduce additional regulation are premature and that the Draft Impact Analysis is flawed due to a lack of real-world understanding and engagement with each sector of the likely costs and benefits of further regulation.

The water sector also finds it difficult to provide a detailed response to a regulatory impact analysis for what is essentially a consultation document rather than actual draft legislation. For example, it is impossible to size the amount of effort required to reply to a definition of 'business-critical data' or to understand what is meant by a 'deficient RMP' without access to the proposed statutory definitions.

Further, the water sector is concerned about the very tight timeframes for the industry to respond to the new regulatory proposals and the regulatory impact statement. These have seriously limited our ability to undertake adequate consultation within our industry and with our jurisdictional (State and Territory Governments and local government) owners and regulators.

Support for some proposed measures

Nevertheless, as we have noted below, the water sector is supportive of some of the Government's proposed measures. Our previous submission with respect to the policy proposal is attached for convenient reference.

The sector's response to this regulatory impact assessment is framed by our response to the Government's policy proposal.

2. Response to the three identified problem elements and consultation questions

Problem 1.1: There is a growing number of cyber incidents which impact non-operational data storage systems held by critical infrastructure entities, which can often be a point of entry for malicious actors.

The Government's proposed response to this problem is to create a new definition within the SOCI Act for "business critical data" (p. 6). While the water sector strongly supports the policy objective of appropriately protecting information and data storage systems, we are concerned that the proposed definition is much too broad. This would cause three significant problems:

1. Such a broad definition would create significant ambiguity and confusion, making it difficult to comply with.
2. The definition would compromise or complicate the capability of an individual water business to use business-critical data for legitimate purposes, such as its own operations, or share the data with trusted third parties.
3. The definition would result in significant expense for organisations in data risk management and remediating data risk for data that has little material value to a cyber threat actor. This risk is significant for many organisations and in many instances may be cost prohibitive to fully address.

It is also unclear what is meant by a data storage system. For example, does this refer to a data centre, such as a GOVDC, or does it also include the connections between a data centre and local servers? The latter will give rise to a high degree of complexity in terms of assessing overall system vulnerability.

The hypothetical scenarios presented in the consultation document suggest that the industry is unsure what loss of data should be reported or incorporated into a Critical Infrastructure Risk Management Plan (CIRMP). While this is possible, the uncertainty is caused by the breadth of the definitions for 'business-critical data' and 'non-operational data storage systems'.

Further broadening the definition of business-critical data has the potential to broaden the interpretation of SOCI Act requirements to cover the entirety of a water business's operations. While a wider definition may increase some reporting and apparent situational awareness for the Government, it is unclear from the scenarios how a widened definition of business-critical data, without a balancing need to assess the potential significance of any data loss, would contribute to enhancing cyber-resilience and coordinated response action. What is more likely to occur is development of a 'report it all' policy to avoid compliance action. This will simply result in an increase in reporting noise to Government, unfiltered and lacking context and priority, creating an administrative burden on Government rather than enhanced risk mitigation and timely response. It will also create potential conflicts between different reporting obligations across multiple levels and branches of government.

Problem 1.2: Businesses often face difficulties responding effectively in the aftermath of critical infrastructure incidents because of legal risks and government's limited ability to support with post-incident consequence management.

The scenarios suggest that post-incident consequence management is limited by the industry's response and coordination capabilities. For this reason, the water sector has partially supported the expansion of consequences management powers, however, the scenarios underplay the potential for poorly judged or hasty incident response actions to create additional hazards.

To reduce the possibility of these outcomes the sector recommended that:

1. 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.
2. The local state or territory authority controlling the affected entity should be included in the consultation process and decision chain.
3. The entity cannot be required to comply with a direction if the entity advises that it cannot in good faith comply (e.g., for public health, safety, environmental, regulatory or operational reasons), or if the direction conflicts with another ministerial (Federal or State) direction.
4. 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.
5. In complying with the direction, the responsible entity must be indemnified from criminal as well as civil liability.

Water sector entities are regulated by State and Territory jurisdictions, and most are owned by State and Territory or local governments. The Minister must respect jurisdictional arrangements and work with jurisdictional owners and regulators when engaging the water sector. This is especially important if the Minister wishes to invoke the consequence management powers and issue directions.

Problem 1.3: When an entity is unwilling to comply with the regulator's recommendations to enhance an RMP, there is no ability for the regulator to issue a direction that the entity remedy the deficient RMP.

The sector strongly disagrees with the contention that a regulated water entity would not in good faith seek to address a Government's concerns that a CIRMP was deficient. Ignoring the fact that such an action would demonstrably create a significant reputation risk for the entity, it would also likely void or compromise corporate insurance arrangements, increase civil liability, potentially impact licencing conditions, and exceed the business' risk tolerance. In addition, most water sector entities are government-owned entities, and it is unlikely that government owners would tolerate such a decision.

We note that the impact analysis provides no examples of such an event having occurred or even an example of unwillingness by the water sector to voluntarily comply with Government risk-mitigation advice, particularly if that advice was in relation to a specific threat. It is the sector's lived experience that the water utilities will willingly act on government threat advice, even if the advice is not specifically addressed to the sector or is general in nature.

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

There are three significant implications of this proposed measure:

1. First, it is not clear how the regulator would assess a CIRMP to determine that it is deficient. All major water utilities have CIRMPs in place that are consistent with the formal risk appetite statements and risk management policies approved by their Boards, and these are aligned with relevant Australian standards as required by the CIRMP rules. Without a clear definition of what is adequate versus what is deficient the determination about required changes is likely to be subjective and provide additional technical and regulatory burden. A clear definition should be developed in consultation with each relevant sector.
2. Second, if the regulator invokes legislative powers to determine the adequacy or deficiency of CIRMPs, depending on the level of detail defined, this can effectively transfer to the Commonwealth Government responsibility and accountability for the content of the CIRMP's, including potential liability for consequences should its determination prove harmful to the entity or stakeholders, or have significant funding implications.
3. Third, as water services are predominantly owned by State or local governments, the proposed measure has the potential to create complexity, confusion, and conflict between governments.

Nevertheless, the water sector accepts that changes in the security environment may require changes to an entity's 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 before issuing a direction.
- During 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, the Commonwealth Government must be clear that it takes full responsibility and accepts all liabilities 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 from the entity, the consequential liability and damages arising should accrue to the Commonwealth Government.
- The financial implications of a direction should be transparent to jurisdictional price-setting structures and allowed for in cost-recovery directly or indirectly.

The creation of a penalty clause for non-compliance further undermines the Government's commitment to a collaborative rather than coercive approach to strengthening critical infrastructure security. Given that the Department would only be able to review an entity's CIRMP 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 relationship capital building the industry's confidence in CISC's regulatory philosophy the proposal of this amendment, without appropriate contextualisation, risks undermining the sector's trust in the CI security arrangements.

3. Response to net benefit assessment

We note the Government is considering further legislative and regulatory action, despite the fact that the 2021 and 2022 amendments to the Act and the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 have only recently come into force and the first compliance reports have not yet been submitted to the Department.

In considering the sector's experience implementing the SOCI Act, its amendments, and regulations, we note the Act is complicated and the Government has not provided a comprehensive or compelling analysis of the costs, benefits, and outcomes the previous reforms have delivered. This suggests that the benefits of the past reforms were either overstated or have under-delivered.

At best, it is too early to assess costs and benefits because the recent legislative changes are still being responded to. The policy intent was to uplift CI security. It is difficult to understand how the Government has been able to assess the effectiveness of existing measures and determine that they have been ineffective in delivering on the policy objective of a whole-of-nation uplift in critical infrastructure security, within such a short time of the changes being implemented. It is premature to implement additional changes in the absence of this information.

Nevertheless, as noted in our response to the Government's policy proposals, the water sector does believe there are potential benefits in some (but not all) of the proposed measures. We have identified these measures below, and we have previously provided a detailed response, which we have attached for completeness.

The water sector believes the Government should maintain the status quo until sufficient real-world experience has generated the evidence to support a compelling argument for further change.

The interaction between State ownership, State economic regulation, and Commonwealth critical infrastructure security regulation

Water sector entities are regulated by State and Territory jurisdictions, and most are owned by State and Territory or local governments. There is a significant risk of regulatory duplication between the States and Federal Governments with some of the measures proposed, creating inter-jurisdictional complexity, confusion, and conflict. We are concerned that the proposed amendments and the cost-benefit analysis do not adequately consider these issues.

Under National Competition Policy the water sector operates in a highly cost-regulated environment. Regulators at arm's length from jurisdictional owners issue regulatory determinations that set overall capital and operating budgets typically on a three- to five-year budget cycle. Water utilities are required to price services to meet these budgets.

Frequent changes to the SOCI legislation cause significant difficulties for regulated entities for the following reasons:

1. Capital and operating funding allocations are locked in through the water utility pricing determination for the regulatory cycle for three to five years. Whilst it is possible for regulated entities to renegotiate their pricing submission to accommodate statutory changes that are introduced during a current regulatory period such changes involve significant time and cost, and must be agreed with the State or Territory economic regulator. Economic regulators have historically demonstrated a strong reluctance to pass through regulatory costs into prices except in rare circumstances. A lead time of 2-3 years is suggested as appropriate to enable implementation costs can be built into future regulatory submissions.
2. In a political environment that is highly conscious of cost-of-living pressures, it is difficult for jurisdictional owners to support water utilities with price increases to accommodate increased compliance costs.

4. Response to proposed policy options

Option 1. Maintain the status quo

The water sector has indicated support for some of the Commonwealth Government's proposed measures, particularly:

- the introduction of secure-by-design standards (Measure 1);
- establishment of a Cyber Incident Review Board (Measure 4);
- changes to the protected information provisions (Measure 7); and
- consolidation of telecommunications security requirements under the SOCI Act (Measure 9).

The water sector provided in-principle support for Measures 3 and 5, with a number of recommendations provided to enhance the proposed measures. However, Measures 2 and 8 were not supported, and Measure 6 was partially supported, primarily because the proposed measures created regulatory duplication and inappropriately impacted on the capability of an individual water business to appropriately manage risk.

Option 2. Amend the SOCI Act

As noted in the sector's response to the Government's policy proposals, the sector sees value in a number of the proposed measures and accepts that some legislative change would be required to implement many of the measures, in particular Measures 7 and 9.

However, the Government is proposing other amendments to:

- ensure capture of 'business-critical data' in relevant definitions in the Act and all CIRMP rules;
- legislate an all-hazards power of last resort, for use by the Minister where there is no existing power available to support a fast and effective post-incident response; and
- introduce a formal, written directions power to address seriously deficient RMPs.

The water sector has significant concerns about these proposals.

(a) 'Business critical data'

As noted above, very broad terms such as 'business-critical data' can introduce significant uncertainty and significant costs without any significant benefits, such as a reduction in actual risk, if terms are broadly drafted to include secondary data or data storages that are not actually business critical.

(b) All hazards power

Further, the introduction of additional powers to compel an entity to change or amend a CIRMP, compulsory reporting of ransomware and enhanced consequence management powers regulations represent a significant increase in Government power. They do not appear to have been drafted with sufficient regard to real-world experience and are not balanced with considerations of proportionality, cost-effectiveness or transference of risk between Government and industry.

(c) Direction power

Finally, the assumption that a Government direction can be issued for a complex system of highly interconnected and inter-operating critical infrastructure entities without strong sector engagement to avoid any adverse consequences for the entities and the Australian public is naively optimistic.

Missing from the regulatory impact analysis are the potential costs of a poorly considered direction, particularly a direction that results in additional potential hazards or realised risks. To avoid these risks it is essential that there is strong sector engagement, and discussions with affected water businesses, taking into account information and caveats provided by those businesses.

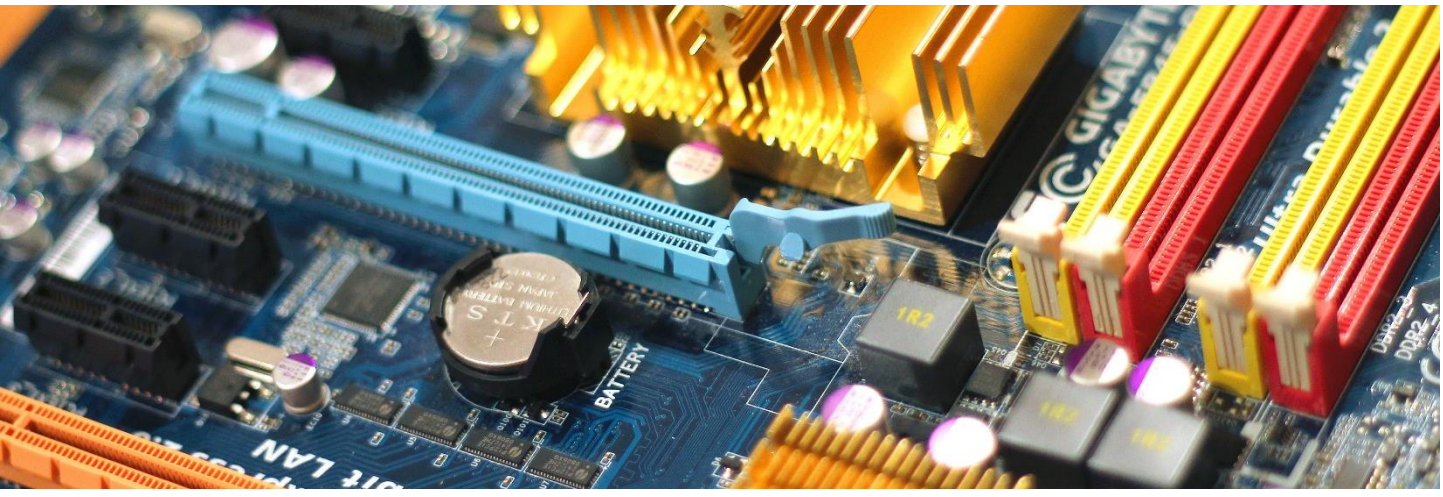
Option 3. Enhance collaboration with industry, through the use of the TISN

It is the water sector's view that the potential for significant benefits of cooperation and engagement through the TISN has not been fully realised by the Government.

Since the inception of the TISN following the 2003 Bali bombings the water sector has found the TISN arrangements have been an effective vehicle for engagement, development of shared-situational awareness, the communication of threat intelligence, and holistic risk mitigation. While TISN membership is not universal, within the water sector all the major utilities are represented and work collaboratively to achieve significant sectoral resilience. A similar level of collaborative maturity across other sectors would deliver a demonstrable uplift in critical infrastructure resilience and security with minimal need for coercive regulatory measures.

A significant further level of maturity would also be achieved by actively supporting cross-sector arrangements through the TISN targeting areas such as jurisdictional situational awareness and sector interdependencies, such as cross-sector supply chains.

The benefits of using the Critical Infrastructure Advisory Council and TISN, particularly its agility in responding to matters, may significantly exceed the benefits of regulation in a more agile and adaptive manner.



CONCLUSION

The water sector appreciates the opportunity to provide feedback on the draft impact analysis, despite our concerns about the limited time available for consulting within the industry nationally, and with our jurisdictional owners and regulators.

In summary, our principal concerns with respect to the proposed regulatory changes are:

1. The current regulatory impact analysis is actually a regulatory options discussion paper. The water sector believes that a formal Regulatory Impact Analysis should be provided for the selected final option.
2. Definitions (e.g. ‘ business-critical data’, ‘non-operational data storage systems’) have not been finalised, so it is impossible to comment on their potential cost impact. The wording used in the proposal suggests a very broad categorisation of data and systems. This could involve very significant costs to the water industry for protection of what is ultimately low-value data, introduce significant constraints to legitimate business as usual working relationships with data service providers and other third parties, and create potential conflicts with reporting obligations to jurisdictional owners.
3. A power to manage consequences is welcomed, however, as water sector entities are themselves government-owned, and often responsible to State and Territory ministers, there is potential for significant inter-governmental conflict if the process is not carefully designed. There should be exemptions for non-compliance that is consistent with industry good practice. There must also be acceptance by the Commonwealth Government that when it issues a direction, it is also accepting the practical consequences of taking responsibility for command, control and coordination of an incident, including financial consequences. Finally, entities responding to a direction must be protected from criminal and civil liability arising from compliance.
4. It is unclear what would make an RMP deficient, beyond a simple failure to draft a CIRMP in such a way that it explicitly addresses all aspects of the CIRMP rules. The Commonwealth Government has not provided any guidance that would enable an entity to assess whether its CIRMP was adequate or deficient. Further, CIRMPs are consistent with formal risk appetite statements and risk management policies at the entity level. If the Commonwealth then directs an entity to alter its CIRMP, and therefore its risk management program, this cuts across the principle that industry knows best how to manage its risks. In instances when the Commonwealth provides a detailed direction to modify a CIRMP there is also a potential that this transfers risk to the Commonwealth in relation to the consequences of directing an entity to manage risk in a specific way. To avoid these issues the water sector requests clear guidance regarding the assessment of CIRMP adequacy.
5. While some measures are supported, industry remains concerned that the existing measures have not been given sufficient time to work. The rapid introduction of new legislation also makes it difficult to assess the costs and benefits of existing or proposed new measures.
6. Finally, the Government does not appear to be harvesting the value of existing collaborative arrangements through the TISN. Encouragement of best practice through the TISN could result in industry compliance that is more cost-effective, more impactful, and more adaptable and agile in response to the developing security environment than a regulatory-driven approach.

We also wish to highlight the following water sector-specific issues which can impact upon the sector's ability to implement the proposed reforms.

1. The sector operates largely under ownership of, and regulation by, the States and Territories. This environment already brings with it a range of statutory risk management obligations, incident reporting, and assurance measures.
2. In the first instance, any escalation to and assistance from government to mitigate significant security-related events is to State government emergency management frameworks. Federal support and assistance is provided through State structures, not directly.
3. There is a significant risk of regulatory duplication between the States and Federal Governments with some of the measures proposed, potentially creating unhelpful complexity, confusion and conflict. We are concerned that the cost-benefit analysis does not adequately consider these risks.
4. The strict economic regulation under which water entities operate makes it very difficult to accommodate increased compliance costs within current regulatory cycles.
5. Finally, the water businesses manage complex systems that require highly sophisticated and well-designed risk mitigation measures. Therefore a risk mitigation measure that is issued without due consideration of how the water system operates, its interdependence, potential second and third tier consequences for the system as a whole, is likely to have disproportionate or unexpected consequences. We are not convinced that the current analysis has fully considered these costs.

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