WATER SERVICES
ASSOCIATION OF AUSTRALIA

Submission to the Independent Review of the *Security of Critical Infrastructure Act 2018*

December 2025

Submission to the Independent Review of the *Security of Critical Infrastructure Act 2018*

[redacted]

[redacted]

This submission can be published in the public domain.

Disclaimers

This document represents the consensus position on key issues for water utilities members of the Water Services Association of Australia (WSAA) and the Water and Sewerage Sector Group (WSSG) across Australia. This document does not reflect the views of, and is not endorsed by, any Australian Government members of the Water and Sewerage Sector Group.

This submission complements any individual submission from Australian water utilities, but it does not override any individual water utility submission, which should be assessed on its merits.

This water sector submission neither represents the response, nor views of the wholly Western Australian Government owned ‘Water Corporation’ due to regulatory duplication and significant unnecessary regulatory costs enlivened by misaligned regulatory requirements.

Contents

Introduction

The water sector welcomes the opportunity to provide a submission to the Independent Review of the *Security of Critical Infrastructure Act 2018* (SOCI Act). As providers of critical water and wastewater services, the sector fully supports the Government's policy objective of delivering an uplift of security and resilience standards.

As one of the sectors' first regulated under the 2018 version of the SOCI Act, the water sector is well placed to provide useful insights into the operation of the:

- primary legislation;
- subordinate rules and regulations;
- interaction of the SOCI Act with other legislation; and
- associated Government guidance provided to the water sector, as critical infrastructure protection and resilience has grown in national importance.

The water sector's perspectives on the SOCI Act are unique as the sector is mature, a critical interdependency for all other SOCI-regulated sectors, non-competitive, and largely government-owned. In this submission we consider the questions posed by the Independent Reviewer, Dr Jill Slay AM:

- Is the SOCI Act achieving its intending objectives?
- Is the SOCI Act functioning as intended?
- Is the SOCI Act having any unintended consequences?
- Are there are any new or emergent threats the SOCI Act is unable to manage to its current form?

We provide feedback in response to these questions and make 10 recommendations for the Independent Review to consider.

Recommendations

The water sector makes the following recommendations to the Independent Review of the *Security of Critical Infrastructure Act 2018.*

Recommendation 1: Consider removing the obligation to provide operational and technical-level ownership and control from Part 2 of the SOCI Act, moving the obligation to Part 2A as part of the annual critical infrastructure risk management program reporting requirements.

Recommendation 2: Permit entities declared under Sections 51, 52A and other associated private declaration provisions, to disclose this information to other critical infrastructure entities for the purpose of achieving the SOCI Act's objectives.

Recommendation 3: Provide a general defence against prosecution under competition law for regulated entities that cooperate and collaborate for the purpose of achieving objective b of the SOCI Act.

Recommendation 4: Review the SOCI Act's penalty provisions and consider providing a defence against regulatory action for entities providing information to the Government in good-faith and to advance the objectives of the SOCI Act.

Recommendation 5: Review the SOCI Act's power to enable the timely and coordinated dissemination of intelligence on national security risks targeted at entities and sectors that sector security matches the dynamic threat.

Recommendation 6: Review the SOCI Act's risk definitions to closer align with ISO31000 and established risk management practices along with the development of sector-specific rules to better define material risk at a critical infrastructure sector level.

Recommendation 7: Amend the SOCI Act to include provisions that entities subject to the SOCI Act reasonably consult to ensure their operations do not create a material risk to other SOCI Act regulated entities.

8Recommendation 8: Amend the objective of the SOCI Act to explicitly focus on enhancing national critical infrastructure resilience through risk management, business continuity planning, and security-threat assessment and risk mitigation.

Recommendation 9: Include the chemical sector in SOCI legislative arrangements to reflect the chemical sector's national importance and address potential systemic vulnerabilities for the critical infrastructure enterprise.

Recommendation 10: Review and simplify the protected information provisions to facilitate sharing of threat, development of shared situational awareness, and collaborative risk mitigation arrangements.

Is the SOCI Act achieving its intended objectives?

The Government's policy objective is achieving a measurable uplift in national critical infrastructure security. While the water sector has always focused on ensuring water and wastewater services are delivered safely and securely, with appropriate risk management practices; introduction of the SOCI Act, and its subordinate rules and regulations, has provided a legislative basis for water sector entities to invest in enhanced security outcomes.

However, the SOCI Act provides only a limited foundation for building sector resilience. The policy objective cannot be achieved without additional support measures including:

- sector-specific rules;
- development of a whole-of-government, and/or a whole-of-nation resilience strategy; and
- holistic regulatory alignment, supported by a financial investment by government to address priority risk mitigation measures.

This is particularly important in the contemporary dynamic security environment.

Considering the six specific objectives of the SOCI Act (Section 3), the water sector provides the following insights:

- Critical water assets are government owned and operated. Consequently, the SOCI Act is largely irrelevant for the water sector in terms of improving transparency of the ownership and operational control of critical infrastructure (Objective a).
- There is no evidence that the SOCI Act has measurably improved intergovernmental cooperation (Objective b).
- Part 2A adequately addresses the objective for responsible entities for critical infrastructure assets to identify and manage risks relating to those assets. However, the inclusion of multiple overlapping penalty provisions, without providing a defence for entities demonstrably acting in good-faith to comply with the objectives SOCI Act, can result in over emphasis on compliance compared to practical risk mitigation (Objective c).
- The water sector considers the provisions for enhanced cyber security obligations are appropriate. However, an amendment allowing entities declared a 'system of national significance' to reveal that fact to other SOCI-regulated entities would enhance critical infrastructure security resilience and assist with the management of cross-sector interdependence (Objective d).
- The water sector supports the inclusion of telecommunications assets into the SOCI arrangements. However, the right of access for installation and maintenance, granted by the *Telecommunications Act 1997*, has been problematic for the water sector (Objective da).
- Unlike commensurate aviation and maritime transport security legislation, the SOCI Act does not include any penalties for acts of unlawful interference with critical infrastructure. Creating penalty

provisions for acts of unlawful interference with critical infrastructure would provide a signal to the community, critical infrastructure stakeholders and the judiciary, the priority that government has placed on the protection of critical infrastructure (Objective e).

Objective a: Improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks Section 3(a)

Critical water assets (defined in Section 4) are government owned and operated. Consequently, for the purpose of this objective, the SOCI Act is largely irrelevant for the water sector. Requiring water asset owners and operators to provide and maintain ownership and control information is therefore unnecessary. Nevertheless, the sector acknowledges there is value in the Federal Government having a consolidated national register of critical infrastructure data.

The sector can see some value in providing information on outsourced and offshored functions for risk identification purposes, however, the water sector questions if the information is for this purpose, as little to no risk mitigation information has been provided by Government based on the information collected under these provisions. Finally, as the information that must be reported under these obligations, in particular IT and OT-related services changes regularly, the obligation to update this information within 30 days of the change, with an associated penalty provision for non-compliance, places an unnecessary regulatory burden on industry. With no demonstrable benefit provided in return. The water sector considers that the Government's risk mitigation outcomes could be equally delivered through including of any ownership and control changes in the annual critical infrastructure risk management program reporting regime.

RECOMMENDATIONS

Recommendation 1: Consider removing the obligation to provide operational and technical-level ownership and control from Part 2 of the SOCI Act, moving the obligation to Part 2A as part of the annual critical infrastructure risk management program reporting requirements.

Objective b: facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks Section 3(b)

There is no evidence that the SOCI Act has measurably improved intergovernmental cooperation. Industry is entitled to expect that that the Department of Home Affairs would work to operationalise the SOCI Act in a way that encourages this. However, there is still a view among some state and territory governments, and pricing regulators, that the national security and national resilience goals of the SOCI Act are a matter for the Commonwealth. This is a substantial challenge for cost-controlled state-owned corporations that depend upon state pricing authorities to approve, and in effect underwrite, the cost of the security uplift born of obligations in the SOCI Act.

As state and/or local government owned and non-competitive organisations, water utilities have long collaborated on security, safety and operational issues. Consequently, the SOCI Act has not materially contributed to an improvement in collaborative risk management. In-fact the inclusion of penalty provisions within the Act has impacted industry's confidence in sharing risk information with Government. In addition, the secrecy provisions and penalties provided under Part 4, Division 3 (specially Section 45), and penalties for unauthorised disclosure of a Minister's private declaration of a critical infrastructure under Sections 51 and 52A, has demonstrably impacted the water sector's capacity and confidence to work collaboratively on risk mitigation measures. Although the

Department of Home Affairs has attempted to alleviate these concerns by providing advice on its approach to compliance, this is non-binding and not underpinned by any provisions in the SOCI Act or the related rules and regulations.

While less of an issue for the water sector, we also note that the SOCI Act provides no defence against accusations of collusion or non-competitive behaviour made under consumer and market protection laws, even if the accused entities have been acting in good faith to enhance critical infrastructure security and resilience. The sector notes a number of practical examples where the Government has had to engage with competition regulators to mitigate this risk during high profile and significant events. Amending the SOCI Act to include a defence against accusations of collusion and anti-competitive behaviour would materially enhance intra and cross-sector cooperation.

RECOMMENDATIONS

Recommendation 2: Permit entities declared under Sections 51, 52A and other associated private declaration provisions, to disclose this information to other critical infrastructure entities for the purpose of achieving the SOCI Act's objectives.

Recommendation 3: Provide a general defence against prosecution under competition law for regulated entities that cooperate and collaborate for the purpose of achieving objective b of the SOCI Act.

Objective c: Requiring responsible entities for critical infrastructure assets to identify and manage risks relating to those assets Section 3(c)

The water sector considers that Part 2A adequately addresses the objective for responsible entities for critical infrastructure assets to identify and manage risks relating to those assets. However, the inclusion of multiple overlapping penalty provisions, without a defence for entities' demonstrably acting in good-faith to comply with the objectives of the SOCI Act, may result in an over emphasis on compliance over risk mitigation.

For example, Section 30AE requires entities to review the program on a regular basis, without clarification of what constitutes a regular basis, while Section 30AF requires entities to take all reasonable steps to ensure the program to ensure it is up to date. Failure to comply with each Section is subject to a civil penalty of 200 penalty units. These penalties can be applied even though these provisions are largely identical. However, there is no defence for an entity failing to comply with these obligations.

We note that many of the risks that responsible entities are obliged to identify are national security risks dynamically originating from foreign actors. This obliges entities to individually identify and manage national security risks for which they have limited information to act on has created a highly diverse and divergent range of risk management programs and practices within the sector.

The issue of divergence is caused by the SOCI Act's material risk and relative impact provisions, which are not harmonised with the international risk standard ISO31000 or widely understood industry approaches to risk management practice, such as So Far as is Reasonably Practicable (SFAIRP) and As Low as Reasonably Practicable (ALARP).

While the sector understands and supports the Government's desire to provide entities with flexibility in how they define and treat risk, closer alignment of the legislative provisions with ISO31000 combined with additional guidance on the definition of material risk would be beneficial. Given the diversity between and within the critical infrastructure sectors, this could most effectively be delivered by sector-specific rules that better define what constitutes a material risk.

RECOMMENDATIONS

Recommendation 4: Review the Act's penalty provisions and consider providing a defence against regulatory action for entities providing information to the government goof faith and to advance the objectives of the Act.

Recommendation 5: Review the Act's power to enable the timely and coordinated dissemination of intelligence on national security risks targeted at entities and sectors that sector security matches the dynamic threat.

Recommendation 6: Review the Act's risk definitions to closer align with ISO31000 and established risk management practices along with the development of sector-specific rules to better define material risk at a critical infrastructure sector level.

Objective d: Imposing enhanced cyber security obligations on relevant entities for systems of national significance in order to improve their preparedness for, and ability to respond to, cyber security incidents Section 3(d)

The water sector considers the provisions for enhanced cyber security obligations are appropriate. However, an explicit provision that allows entities declared 'a system of national significance' to disclose this status to other critical infrastructure entities for the purpose of achieving the objectives of the SOCI Act (facilitating greater information sharing and collaboration), would contribute to enhanced critical infrastructure security resilience. For example, a data centre declared to be a system of national significance, could inform its water services provider, for the purpose of working collaboratively to ensure continuity of services to the data centre during emergencies.

The water sector notes these is a level of de-facto declaration through the establishment of the system of national significance sector group within the Trusted Information Sharing Network and Critical Infrastructure Advisory Council arrangements.

To address this feedback, we refer to Recommendation 3.

Objective da: Imposing enhanced security obligations on responsible entities for critical telecommunications assets Section 3(da)

The water sector supports the inclusion of telecommunications assets into the SOCI arrangements. However, the right of access for installation and maintenance, granted by the *Telecommunications Act 1997*, has been problematic for the water sector. For example, telecommunications entities, or entities acting on their behalf, exercising a right of access have impacted the safe and secure operation of water sector assets.

RECOMMENDATIONS

Recommendation 7: Amend the SOCI Act to include provisions that entities subject to the SOCI Act reasonably consult to ensure their operations do not create a material risk to other SOCI Act regulated entities.

Objective e: Providing a regime for the Commonwealth to respond to serious incidents relating to critical infrastructure assets Section 3(e)

Unlike commensurate aviation and maritime transport security legislation, the SOCI Act does not include any penalties for acts of unlawful interference with critical infrastructure. Consequently, the SOCI Act imposes obligations on the owners and operators of critical infrastructure to prevent or

mitigate material risks to the operation, reliability or integrity of the critical infrastructure asset but threat actors can seek to disrupt critical infrastructure without any specific penalty. While these acts may be prosecuted under other legislation, creation of penalty provisions for acts of unlawful interference with critical infrastructure would better signal the Government's policy intent and prioritisation of the issue.

Is the SOCI Act fit for purpose and functioning appropriately?

As a foundation for delivering an uplift in national critical infrastructure security the SOCI Act, and its subordinate rules, is broadly functioning appropriately. However, the water sector considers that the SOCI Act over-emphasises concepts of 'security' and mitigation of specific threats, rather than delivery of national critical infrastructure resilience, through holistic all-hazard risk management.

While promotion of all hazard's risk management is implicit, the SOCI Act and the subordinate rules' explicit provisions are focused on security risk management. Consequently, entities often focus on the 'SOCI pillars' of cyber security, supply chain security, personnel security, physical security and natural hazards, rather than adopting resilience measures necessary to ensure the continued operation of critical infrastructure in the face of dynamic and evolving threats.

The water sector considers that this shortcoming could be addressed by amending the object of the SOCI Act to explicitly focus on enhancing national critical infrastructure resilience through risk management, business continuity planning, and security-threat assessment and risk mitigation.

RECOMMENDATIONS

Recommendation 8: Amend the objective of the SOCI Act to explicitly focus on enhancing national critical infrastructure resilience through risk management; business continuity planning; and security-threat assessment and risk mitigation.

Is the SOCI Act having any unintended consequences? Are there any gaps or amendments required to the SOCI Act?

As noted in our feedback on Objective c, the SOCI Act is not aligned with well-understood industry approaches to risk management, which has created confusion and an unnecessary focus on compliance. This appears to be a result of attempts to implement a prescriptive and legislative approach to critical infrastructure risk management, which undermines the Government's policy objective of a seeking collaborative and adaptive implementation of risk management practices across industry.

By accepting the principle that industry wants to work collaboratively with Government to mitigate risks, many of the provisions and penalties in Parts 2A and 2AA could be: simplified; moved to the rules; or withdrawn and replaced by guidance material and advice. This model was implemented successfully by the Attorney-General's Department as the original convenor of the Trusted Information Sharing Network. The Attorney-General's Department was viewed by industry as a collaborative partner rather than a regulator. The water sector notes that failure to follow formal Government advice often creates other risks for businesses such as invalidation of insurance coverage, which is a far more powerful incentive for risk mitigation. To address this feedback, we refer to Recommendation 5.

In respect to gaps in the SOCI Act, the water sector has long advocated for the inclusion of the chemical sector into the SOCI legislative arrangements. For the water sector, chemicals are critical for water and wastewater treatment. Chemical supplies are also critical for the defence, agriculture and health sectors. However, despite these demonstrated interdependences, the chemical sector is not considered a critical infrastructure sector and is not SOCI regulated, creating regulatory misalignment and potential vulnerabilities. The water sector strongly recommends incorporation of the chemicals sector into the SOCI arrangements both to reflect the sector's national importance and to address potential systemic vulnerabilities for the critical infrastructure enterprise.

The use and disclosure of protected information provisions in Division 3 are complex and potentially undermine cooperation and information sharing with other industry participants. In particular, Section 43E does not allow the entities to disclose protected information to other industry participants (without the approval of the Secretary – Section 43E(2)(b) and (c) and there is no defence provided under Section 46.

RECOMMENDATIONS

Recommendation 9: Include the chemical sector in SOCI legislative arrangements to reflect the chemical sector's national importance and address potential systemic vulnerabilities for the critical infrastructure enterprise.

Recommendation 10: Review and simplify the protected information provisions to facilitate sharing of threat, development of shared situational awareness, and collaborative risk mitigation arrangements.

Are there new or emergent threats the SOCI Act is unable to manage in its current form?

The water sector considers that the SOCI Act provides an appropriate framework for responding to new and emerging threats. However, as there is no obligation for regular reviews of the rules (which operationalise the response to threat and risk), there is potential for an ongoing growth in regulatory obligations that have not been reviewed for ongoing relevance and appropriateness.

As the threat environment is highly dynamic, consideration should be given to amending the legislation requiring regular independent reviews of the primary and subordinate legislation. This measure would ensure that the SOCI Act and its enabling rules continue to provide a legislative framework that is commensurate with the contemporary threat environment.

Submitting Organisations

About the Water Services Association of Australia

The Water Services Association of Australia (WSAA) is the peak body representing the Australian water sector. Our members provide water and wastewater 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 water sector. The collaborative approach of WSAA members has led to sector wide advances to national water issues.

About the Water and Sewerage Sector Group

The Water and Sewerage Sector Group (WSSG) is the water industry group that forms part of the Federal Government's Trusted Information Sharing Network. The WSSG comprises the Risk, Security and Resilience experts from across the Australian water sector, 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 water 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 standard and guidelines that will guide the water sector in its approach to operationalising the SOCI legislative requirements.

This submission does not reflect the views of, and is not endorsed by, any Australian Government members of the WSSG.

Contact

WSAA and WSSG welcomes the opportunity to discuss this submission further.

[redacted]

[redacted]