WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER INDUSTRY SUBMISSION

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

1 March 2022

Attention: Committee Secretariat
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

SUBMISSION: Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Adam Lovell	**Brendan Guiney**	**David Cameron**
Executive Director	Executive Officer	CEO
Water Services Association of Australia	NSW Water Directorate	Queensland Water Directorate
Level 9, 420 George Street		43-49 Sandgate Road
Sydney NSW 2000		Albion QLD 4010
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

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

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 NSW Water Directorate

The NSW Water Directorate is an incorporated association representing 89 local government owned water utilities in regional NSW, serving 1.85 million people. The NSW Water Directorate provides independent technical advice to local water utilities to ensure they deliver high quality water and sewerage services to regional communities in NSW. NSW Water Directorate works collaboratively with government and non-government organisations to support, advocate for and enable the needs of local water utilities in NSW.

About Queensland Water Directorate

The Queensland Water Directorate (qldwater) is a business unit of the Institute of Public Works Engineering Australasia Queensland. Their members include the majority of councils, other local and State government-owned water and sewerage service providers, and affiliates.

As the central advisory and advocacy body within Queensland's urban water industry, qldwater is a collaborative hub, working with its members to provide safe, secure and sustainable urban water services to Queensland communities. Major programs focus on regional alliances, data management and statutory reporting, industry skills, safe drinking water and environmental stewardship.

About VicWater

VicWater is the peak industry association for water corporations in Victoria. Their purpose is to assist members achieve extraordinary performance while helping to influence the future of the Victorian water industry. VicWater plays an important role in the Victorian water industry in influencing government policy, providing forums for industry discussions on priority issues, disseminating news and information on current issues to stakeholders, identifying training needs, and the production of performance reports and industry guides.

VicWater is focused on supporting Victorian water corporations and the broader industry in their objective to provide efficient and sustainable water and wastewater services in Victoria.

About Water Sector Services Group

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

The WSSG has been the coordination point for the water sector's response to the SOCI legislation since its inception and will continue to play a lead role in developing the advice; standards; and guidelines that will shape the water sector's approach to operationalising the SOCI legislative requirements.

1. SUBMISSION

1.1 Introduction

The water sector values the opportunity for consultation in relation to the *Security Legislation Amendment (Critical Infrastructure Protection) Bill (SLACIP Bill) 2022* (Cth) and appreciates the Government's consideration and acceptance of a number of suggested changes to the proposed legislation in response to earlier submissions.

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. However, the water sector is concerned that the proposed Bill has an over-reliance on regulatory solutions and government control, which is a demonstrably less effective response to our shared security challenges.

1.2 Feedback on consultation

1.2.1 Inclusivity and timing

The water sector believes that the engagement over the proposed SLACIP Bill was inclusive and wide ranging. However, the timeframes for consultation were extremely compressed, over the Christmas, New Year and January period. A time when the sector is often pre-occupied responding to impacts from natural hazards including fire and flood, across most of the country. Expecting a considered response to all aspects of the Bill and the engagement process during this time should be considered unreasonable given the critical nature of the Bill.

1.2.2 Incorporation of feedback

The sector provided significant feedback on the draft sector specific rules. A number of these comments were incorporated into the SLACIP Bill. However, in terms of comments that were made directly on the provisions of the primary legislation (the Bill), almost none of the sector concerns have been addressed. These concerns are outlined in 1.2.3 below.

1.2.3 Potential regulatory impact

The Bill in its current form does not impose significant additional regulatory costs to water businesses, on the basis that no water business has been identified as a System of National Significance. It is anticipated that declaration of a water business as a System of National Significance is likely to have costs in the order of several hundreds of millions of dollars, based on an understanding of likely cyber security requirements. This cost is currently hidden because the declaration of a System of National Significance is not subject to a regulatory impact statement.

This issue is of particular concern for the water sector as the majority of entities operate under a system of controlled pricing, with cost-recovery actions subject to regulatory approval. If the entity is unable to inform its pricing regulator that it has been declared a System of National Significance, it is unlikely to gain approval to pass on any proposed price rise.

In addition, the sector raises concern any future rules developed and approved under the Ministers rule making power, are currently unable to be costed (because they have not yet been written) and will not be subject to any regulatory impact statement.

1.2.4 Five key themes for the feedback on the Bill

Supply Chain

The legislation as drafted is silent on the Chemical Sector. However, the recent supply chain issues caused by the floods in South Australia have highlighted the criticality of this sector to the resilience of critical infrastructure. The inability to move chemicals across the Nullarbor impacted a number of the critical infrastructure sectors covered by the Act including water and sewerage, food and grocery, and health care and media. Because of this reliance it is suggested that the Chemical Sector should be added to the list of sectors covered by the Security of Critical Infrastructure Act (2018).

Enhanced cyber security obligations for Systems of National Significance

We note the current consideration for declaration of an entity as controlling Systems of National Significance (SONS - Section 52B):

- Consequences of a significant relevant hazard to Australia's social or economic stability, people, defence or national security;
- Interdependencies with other critical infrastructure Assets;
- Other matters considered relevant by the Minister.

The sector reasserts our position from previous submissions that as there are no significant water sector cross-border interdependencies, nor significantly interconnected networks, and the sector operations are inherently resilient, that no water sector entities will constitute *"systems of national significance".*

We welcome the engagement with the First Ministers Office of each State or Territory in the declaration of a SONS because of the State and Territory ownership of virtually all water businesses with greater than 100,000 property connections, who might be called up as SONS. We note, however, that a small number of water utilities captured by the SOCI Act are local government owned. There is currently no provision in the Bill for engaging with Local Government owners. This is an oversight which should be addressed by also requiring engagement with the Jurisdictional owners of the entity prior to any declaration of a SONS.

The sector is also highly concerned with the lack of an appeals process in relation to the Enhanced Security Obligations placed on SONS. The exposure draft provides opportunity to engage with the entity in relation to an Exercise, Vulnerability Assessment or Access to Systems Information. However, there are no checks and balances on what can be required,

nor any opportunity to appeal disproportionate requirements other than through direct application to the Minister.

Cyber Security Exercises

In the event that a water entity is declared a SONS, it is unclear how the overlap between Commonwealth and State coordination agencies will be managed during exercises and incidents. We suggest that Section 30 needs to be revised to acknowledge and clearly articulate the interaction between the DHA and current state-based organisations during a major incident. Failure to do this risks confusion and delays at a time when this can be least afforded.

Protected Information

Highlighting a flaw in the definitions

In the exposure draft there is a fundamental flaw in the recommendations, as follows. Amendments 19 and 20 of the SLACIP Bill propose amendments to the definition of Protected Information – information that cannot be revelated to any external entity without specific permission from the Minister or the Legislation. Amendment 19 inserts a new paragraph (bc) to the definition of 'Protected Information' which indicates that the entire risk management program is protected information. This renders the risk management program unworkable. The risk management program typically covers every aspect of business operations. In day-to-day operations it is essential to be able discuss and refer to elements of the risk management program. These elements are also typically an embodiment of ongoing operational management for both the Entity and any subcontractors. In addition, achieving good practice risk management requires the sharing of key aspects of the risk management plan with auditors and other external parties. Inhibiting this exchange of information will severely inhibit achievement and realisation of good practice risk management. The same logic applies to the proposed insertion at Amendment 20 of the new paragraph (bf).

Paragraph '(bd)' of the proposed amendment to the definition of 'Protected Information' applies to any update or modification to the risk management that is notified under Section 30AG. Any such changes would then need to be isolated and would be unable to be shared or discussed. Again, this action actually inhibits good practice risk management and works against the stated goal of a security uplift.

We recommend that the proposed Amendments 19 and the proposed new paragraph (bf) at Amendment 20 are not adopted into the proposed legislation.

Disclosure to contracted entities

In addition, the water sector notes that water infrastructure operators commonly use contracted entities (i.e. third party contractors) as a fundamental component of their business model. This extends to agreements and “engagements” with academic institutions; international water associations; overseas academic institutions and non-regulatory jurisdictional agencies engaged in risk assessments who are neither contracted to, nor form any part of a Government regulated process, are commonplace across the national and international water sector.

Under the SoCI Act, as amended by the SLACIP Bill, responsible entities for critical water assets would only be permitted to provide contracted entities with 'protected information' for the purposes of the responsible entity exercising its power, or performing its functions or

duties under the SOCI legislation, or otherwise ensuring compliance with the SOCI legislation. The exception to the general restriction to share protected information does not capture the sharing of protected information for the purpose of operating critical infrastructure assets in the ordinary course of business (absent formal approval being sought and obtained which would impose a significant burden on responsible entities and could lead to material operational issues, particularly in emergency circumstances).

To this end, and further and in the alternative to the submission made in respect of the proposed revisions to the definition of 'Protected Information', the water sector submits that section 41 of the *Security of Critical Infrastructure Act (2018)* should be amended so as to confirm the ability of an entity to disclose protected information for the purpose of the proper operation of a critical infrastructure asset or a critical infrastructure sector asset.

a. Insertion after current section 41(b):

> *(b) … ; or*
>
> *(c) facilitating the proper operation of the critical infrastructure asset, or critical infrastructure sector asset, to which that protected information relates.*

This amendment will ensure that entities are able to share protected information for the purpose of ensuring the smooth operation of critical infrastructure assets which may not be directly related to the discharge of that entities functions or under, or ensuring compliance with the SOCI legislation, but is nonetheless required for the safe and proper operation of the relevant asset. This will also simplify the ability for supply chain assurance and ensure consistency in the understanding and approach to fulfilling supply chain obligations, particularly in relation to cyber security.

Disclosure to government

The water sector notes the clarity provided by addition of Clause 43E in relation to the ability to disclose protected information to State, Territory and Federal Ministerial representatives and welcomes the ability conferred under paragraph 2 for the Secretary to consent to the disclosure of protected information to third parties.

However, we note with some concern that a number of water utility companies which are subject to the SOCI Act are, or report directly to, local government entities (i.e., the reporting and responsible entities for critical water and sewerage sector assets and critical water assets – respectively – are primarily local government owned entities, or an agency of the local government itself). Accordingly, the only recourse for these entities to talk to their jurisdictional owners about protected information, on the terms of the SLACIP Bill, would be through a separate Ministerial declaration.

This is an onerous mechanism and is inconsistent with the intended insertion of new Clause 43E. The water sector submits that the wording of Section 43E, should be amended as follows:

a. Insertion of new paragraph (a)(iii) which permits the sharing of protected information to *'relevant local government authorities which have oversight of the relevant critical infrastructure sector to which the protected information relates'*; and

b. Amendment of existing paragraph (a)(iii) to reference '*a person employed as a member of staff of a Minister or local government authority mentioned in subparagraph (i), or (ii) or (iii)*'.

Confusion caused by conflicting risk terminology

- There is inconsistency between the terminology used in the legislation and internationally recognised risk terminology as used by most CI providers. In a crisis, the use of inconsistent terminology between the legislation and CI providers in this manner is likely to cause confusion and result in poor outcomes at the least desirable time. In addition, should a matter concerning interpretation of the Act be presented in the Courts it may be difficult to navigate what is a reasonable interpretation of the terms, given the conflict with internationally accepted risk-management terminology. The following are suggested to address this issue:
  - Clause 30AG 2(d)(ii) is incompatible with international risk terminology as described in ISO 31000. The wording should be modified as follows: *The entity must outline any instances where a hazard had a significant impact on the asset, how the material risk from that hazard was mitigated and any changes to the program as a result of the risk being realized ~~hazard~~.*
  - Clauses 30AH 1(b)(ii), 30AH 9 and 30 AH10 all use the term 'eliminate' when talking about a material risk. This terminology is incompatible with internationally accepted risk terminology as described in ISO 31000. There are only two pathways to the elimination of a (material) risk. The first is to eliminate the threat that gives rise to the risk, which is clearly beyond the ability of a CI asset (and likely government as well). The second is to eliminate ALL vulnerability to that threat, which is almost always impractical and unrealistic. Therefore, the only reasonable mandate on a CI asset is to minimise as far as is reasonably practicable. Anything beyond this is an over investment that gives rise to diminishing returns.
  - The terminology used in 30AH (a) *identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset* is not standard risk management nomenclature and will cause confusion to any risk manager developing a risk management plan consistent with ISO 31000. Such confusion may result in perverse outcomes from attempts to comply with the legislation. All wording should be as clear as possible to avoid this.

    Suggest rewording as 'the risk management plan (the RMP) should identify threat vectors [as opposed to hazards] that could impact adversely the performance of the critical infrastructure asset. The RMP should also document the likelihood and consequence of risks arising from a consideration of those threat vectors. If such a risk is deemed to be material to the asset, then the RMP will need to document a strategy for the management of that material risk.'
  - Clauses 30 AH (b) and (c) confuse hazard with risk. A hazard is a factor that can give rise to a risk. Risk is the likelihood and consequence or impact of the hazard. The wording should be amended as follows:
    - Clause 30 AH (b) *so far as it is reasonably practicable to do so minimise ~~or eliminate~~ any material risk from such a hazard ~~occurring~~;*
    - Clause 30 AH (c) *so far as it is reasonably practicable to do so—mitigate the relevant impact of such a material risk~~hazard~~ on the asset*

Compensation for commercial loss as a result of a direction

Bill 1 as written allows the Secretary to issue Directions to a CI Entity that relate to a critical cyber security incident under authorization by the Minister. These directions

enable access and modification to the operation of digital business systems of the CI entity(s). This includes accessing, altering, copying and deleting data.

The Bill holds the entity not liable for damages in relation to a Direction. However, it does not explicitly allow provision for compensation to be paid to the infrastructure owner for commercial losses, which may accrue to its customers. This defaults to common law principles, where these customers would be expecting a level of compensation. The current wording of the legislation creates uncertainty and risk for owners.

This uncertainty would be addressed by the insertion of the following clause after Section 60:

> ***Compensation for Commercial Loss as a result of a Direction***
>
> *(1) If the operation of this Act in relation to a Direction from the Secretary results in a commercial loss for the Critical Infrastructure Entity, the Commonwealth is liable to pay a reasonable amount of compensation to the entity.*
>
> *(2) If the Commonwealth and the entity do not agree on the amount of the compensation, the entity may institute proceedings in:*
>
> *(a) the Federal Court of Australia; or*
> *(b) the Supreme Court of a State or Territory*
>
> *for the recovery from the Commonwealth of such reasonable amount of compensation as the court determines.*

1.2.5 Support for the Bill

On balance the sector supports the introduction of the SLACIP Bill, ideally taking into consideration the points raised in this submission. Further, the sector would support a formal review of the legislation and associated rules within 12 months of the positive security obligations rules being switched on by the Minister.