WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER INDUSTRY SUBMISSION

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 - Exposure Draft

31 January 2021

Attention: Hamish Hansford
Group Manager
Head – Cyber and Infrastructure Security Centre
Australian Department of Home Affairs

SUBMISSION: Security Legislation Amendment (critical Infrastructure Protection) bill 2022 exposure draft

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]		

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

Submission recommendations and comments

The water sector supports the Security Legislation Amendment (critical Infrastructure Protection) Bill 2022 exposure draft exposure and the Government's policy objective of delivering an uplift of security and resilience standards across a range of critical infrastructure sectors.

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;
- Oher 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. 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 declaration of a SONS.

The sector is also highly concerned with the lack of appeal 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.

Board Attestation

The water sector welcomes the clarity provided by Clause 30AG in relation to a Board attestation regarding the risk management program. Particularly because it calls up the requirement for a Board to attest that the risk management program was up to date and how

the entity managed a significant relevant impact of a hazard on one or more of the assets that:

- Identifies the Hazard
- Evaluates the effectiveness of the program in mitigating the significant relevant impact of the hazard on the assets concerned and
- If the program was varied during the financial year as a result of the occurrence of the hazard – outlines the variation.

Protected Information

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

However, it should be noted that the water sector uses contracted entities that may be covered by the SOCI legislation as a fundamental component of their business model. The current wording of the legislation does not allow contracted entities to disclose protected information to their engaging CI Entity. Allowing this disclosure by contracted entities will avoid potential conflicts of interest between commonwealth requirements and contracted obligations. It 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.

Detailed input for the exposure Draft

- Risk Terminology – there is an 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 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*

- Additional Clause in relation to Bill 1
  - The Bill 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 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.