WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER INDUSTRY SUBMISSION

Security of Critical Infrastructure
Risk Management Program Rules
Nov 2022

18 November 2022

Hon Clare O'Neil MP

Minister for Home Affairs

SUBMISSION: Risk Management Program Rules 2022

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	
(02) 9221 0082	(07) 3855 6119
adam.lovell@wsaa.asn.au	luke.sawtell@urbanutilities.com.au

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

Note: This document represents the consensus position on key issues for water utilities across Australia. This submission complements any individual submission from Australian water utilities, but it does not over-ride any individual water utility submission, which should be assessed on its merits. The 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.

Security of Critical Infrastructure – Risk management program Rules (LIN 22/018) 2022 (draft)

The water sector supports the Government's policy objective of delivering an uplift of security and resilience standards across a range of critical infrastructure sectors and welcomes the opportunity to provide a submission on the proposed Critical Infrastructure Risk Management Program (RMP) rules and supporting advice provided to industry.

1. **General:** the Risk Management Program (RMP) rules and associated guidance material appears to include information requirements that extend beyond what is necessary to comply with industry's obligations under the Act. An example are the additional requirements in the Draft Annual Report Approval form detailed later in this submission.

   Whilst the sector understands that collection of additional information may assist the Department, it is the sector's position the rules and guidance must clearly differentiate between the actions necessary to meet legal obligations and the non-mandatory or voluntary reporting requirements.

   The sector notes that industry will incur additional costs to comply with the RMP rules, which will need engagement and, in most cases, approval by the jurisdictional owners and economic/pricing regulators. Given the rule-making powers granted under the Act, any future rule changes must be minimised to avoid increased costs to the community and potential non-compliance by industry. This is particularly a risk where rules specify adoption of a particular framework that may change over time such as the cyber security frameworks. Any misalignment of the timing and outcomes may result in a conflict between State and Commonwealth entities with commensurate impacts on the public reputation of both and additional compliance costs which the sector may not be able to recover outside of the regulatory pricing periods.

   Recommendation: *That the Department only seek to collect information as required under the Act, to clearly and correctly differentiate between mandatory and non-mandatory reporting and minimise future rule changes*

2. **Regulatory Duplication:** the water sector is predominantly state and jurisdictionally owned and risk is effectively managed through state and jurisdictional processes. Therefore, the RMP arrangements should be explicitly designed to complement not duplicate these arrangements.

   - Where jurisdictional regulations exist, these should take precedence over the SOCI obligations.
   - Misalignment of definitions and terminology both within the Act and existing jurisdiction regulations is adding to increased cost and complexity and creating a risk of non-compliance. An example is the descriptions of critical asset vs critical site vs critical component. This appears to be intended as a diminishing hierarchy. However, terminology may be applied differently across the sector and across different sectors leading to vastly different RMP approaches and outcomes. A second example are the terms "proper function" (used in the definition of "critical component" in the Act) or "impairment" (Section 5a of draft Risk Management Program Rules).

- The current rules expose water businesses to reputational, security and regulatory conflict due regulatory duplication. If this cannot be rectified, then the RMP rules will need to state which rules have primacy to avoid the potential for a costly legal challenge in the future.

Recommendations:

- *That the Department provide further guidance on the terms outlined here to ensure consistent application of the Rules.*
- *PSO rules to be amended to explicitly acknowledge the primacy of state and jurisdictions regulatory regimes as the basis for the development of RMPs and the Department's approach to regulation.*

3. **Personnel Hazards:** the water sector remains concerned the Department's public assurances that both critical workers or critical positions could be used when managing risks associated with personnel hazards have not been reflected in the draft PSO rules.

   During industry consultations conducted by the Department in late 2021, numerous commitments were given by the Department that industry would have an option to manage personnel hazards by identifying critical positions and/or critical personnel. The rule was promulgated in response to feedback that identification of individuals was more complicated and less effective than identification of a critical position. The commitment was publicly acknowledged in a 'Town Hall' meeting on 25 November 2021 and in the plain language risk management program rules published by the Department. The critical positions option was also noted in the Department's Action Alert Risk Management implementation and uplift advice published on 25 February 2022. Based on these commitments, some utilities have commenced consultation processes with staff and union representatives, which has been subsequently undermined by the draft rules. In support of our position, industry notes that the Federal Government itself has adopted a position-based approach (security assessed positions) to identifying which employees are subject to additional background checking requirements.

   Recommendation: *The water industry supports the clarification offered by the department at the water sector briefing 10 November 2022 and requests this clarification is included in the guidance material. It was stated the risk program requirement is for the entity to provide confirmation that individuals in critical position are being identified and managed. This approached is preferred over the provision of a list of individuals in the critical positions to the Department.*

4. **Supply Chain**

   Supply chain risks are often common to the entire sector and outside the sector's control. The contextualisation of supply chain risk, particularly as many critical suppliers are international, is more effectively undertaken at a Commonwealth level. Given these factors, having each CI entity undertake the risk contextualisation is inefficient and not in the community's best interest.

   In our assessment, the supply chain requirements detailed in the Rules are similar to the requirements of the Modern Slavery Act (2018). Compliance with that Act requires a statement of attainment that is based on a clear set of questions being asked of the supply chain. In addition, to assist organisations comply with the Modern Slavery Act (2018) a list of high-risk regions and countries is provided and regularly updated by the Department of Home Affairs. This is accompanied by a list of high-risk occupations.

For the Supply Chain risks there are two primary risk types. Sourcing and delivery of materials, which can be readily managed through an assessment of the diversity and location of suppliers. The more complicated risk is the cyber security of supplied technologies. It is here that we request guidance from Home Affairs in providing a list of high-risk countries within the supply chain, and a list of high-risk product types. These lists would be used to determine regions or products that require additional due diligence and assessment by CI entities. It is further recommended that the Department of Home Affairs should prepare a template set of questions for CI Entities similar to those for the Modern Slavery Act. This template would ensure a minimum security uplift across all CI entities in relation to supply chains.

Recommendation: *That the Department of Home Affairs looks to provide supporting materials consistent with those developed for the Modern Slavery Act (2018). These include draft supply chain questions, clarity on countries deemed to be a high risk for supply chains either for direct supply or cyber security, along with products that are deemed high risk.*

5. **Physical Security Hazards and Natural Hazards**:

There is a need to modify or remove Section 11.2(d) 'to control access to critical sites, including restricting access to only those individuals who are critical workers or accompanied visitors' because this is unduly restrictive on routine business operations. There are situations when staff from the organisation, who are not critical workers need to access critical sites and need to do so unaccompanied to undertake their work. This section would unnecessarily complicate these operational arrangements and is in impractical in a number of cases. In particular, this requirement is in direct conflict with Schedule 3 of the Telecommunications Framework, which allows carriers and their subcontractors largely unfettered access to landowner's sites.

Recommendation: *The point needs to be removed or substantially modified. These operational risks need to be managed by the CI Asset Owner as appropriate. The current wording severely inhibits the day-to-day operation of CI assets and is unable to be fully complied with unless there are modifications to the Telecommunications Act. If this is retained, provided amendments are made to relevant competing legislation, there will be substantially increased costs in operation of CI which are passed on the community.*

6. **Critical Infrastructure Interdependencies**

Section 7 (2) (e) focuses on interdependencies of critical infrastructure assets which are not necessarily in the entity's control and has the potential to change without the entity's knowledge. It is requested the Department provide clarification on how it expects critical infrastructure owners to comply with this rule.

Recommendation: *This should be clarified in the text to state 'to the extent these interdependencies pose a material risk to the Asset.*

Protected Information Guidance Material - Industry

The sector welcomes the improved clarity provided by the Protected Information Guidance Material – Industry. However further necessary clarifications are detailed below:

- The industry is legally required to publish a range of information related to risks and operational assets. The protected information provisions in the Act particularly in relation to the information contained in the RMP creates confusion and conflicting regulatory obligations. It also affects our ability to undertake our regulatory obligations efficiently. An example is the preparation of pricing regulatory submissions that requires engagement with the community on material risks.

- Documents or information that will be included under the definition of protected information are regularly distributed for the business purposes of organisations that are not included in the allowable disclosure rules in the legislation. In particular, information is shared with consultants, contractors or other utilities. This information may be used to assist the receiving parties discharge their duties or to assist in the uplift of the performance of the sector. Other potential receivers of protected information will include non-commercial research organisations or Dial Before You Dig. While release of information for this purpose may be covered by the provisions of Section 41, the wording of the provision makes this unclear.

- It has been previously submitted 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.

- The linkage and relationship between “sensitive operational information’ and “protected information” is unclear. Clarification is required on whether ‘sensitive operational information’ will be ‘protected information’.

Recommendation: *the entity should be permitted to use protected information for the purposes of undertaking its regulatory functions or primary business operations. This could be achieved in two ways:*

1. *Clarification in the guidance notes of section 41 of the Act which states:*

   “An entity may make a record of, use or disclose protected information if the entity makes the record, or uses or discloses the information, for the purposes of:
   (a) exercising the entity’s powers, or performing the entity’s functions or duties, under this Act; or”…

2. *Amend Clause 5(bc) of the definition of protected information to exclude the RMP.*

Draft Annual Report Approval Form

Section 30AG of the Act and the draft Annual Report Approval Form refers to “a significant relevant impact”. Whilst “relevant impact” is defined in section 8, there is no specific definition of the term “significant relevant impact”.

The Draft Annual Report Approval Form includes a section requiring “an overview of your approach to manage risks”. Section 30AG of the Act does not include this requirement. Can the department provide guidance on legislative power that supports this inclusion in the report or advise if this is voluntary information only.

The Draft Annual Report Approval Form also includes an obligation to ‘provide a description of the critical infrastructure asset(s) covered by the RMP’ as a mandatory section. This is not a reporting obligation under Section 30AG of the Act and this information has already been provided to Government under the Registration form for the Responsible Entity of a Critical Infrastructure Asset, an example of regulatory duplication by the Department. In addition, the mixing of mandatory and non-mandatory reporting is exemplified by the following question: ‘Please provide an overview of your approach and processes to manage risks’ this question is correctly identified on the form as a non-mandatory field.

Recommendations:

- *That guidance is provided on how the inclusion of the word “significant” alters the definition of “relevant impact”.*
- *The Department of Home Affairs provide guidance on the legislative power that supports the inclusion of the following requirements in the rules or advise if this is voluntary information only:*
  - *‘an overview of your approach to manage risks’*
  - *‘provide a description of the critical infrastructure asset(s) covered by the RMP’*

Appendix 1: Submitting Organisations

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 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.