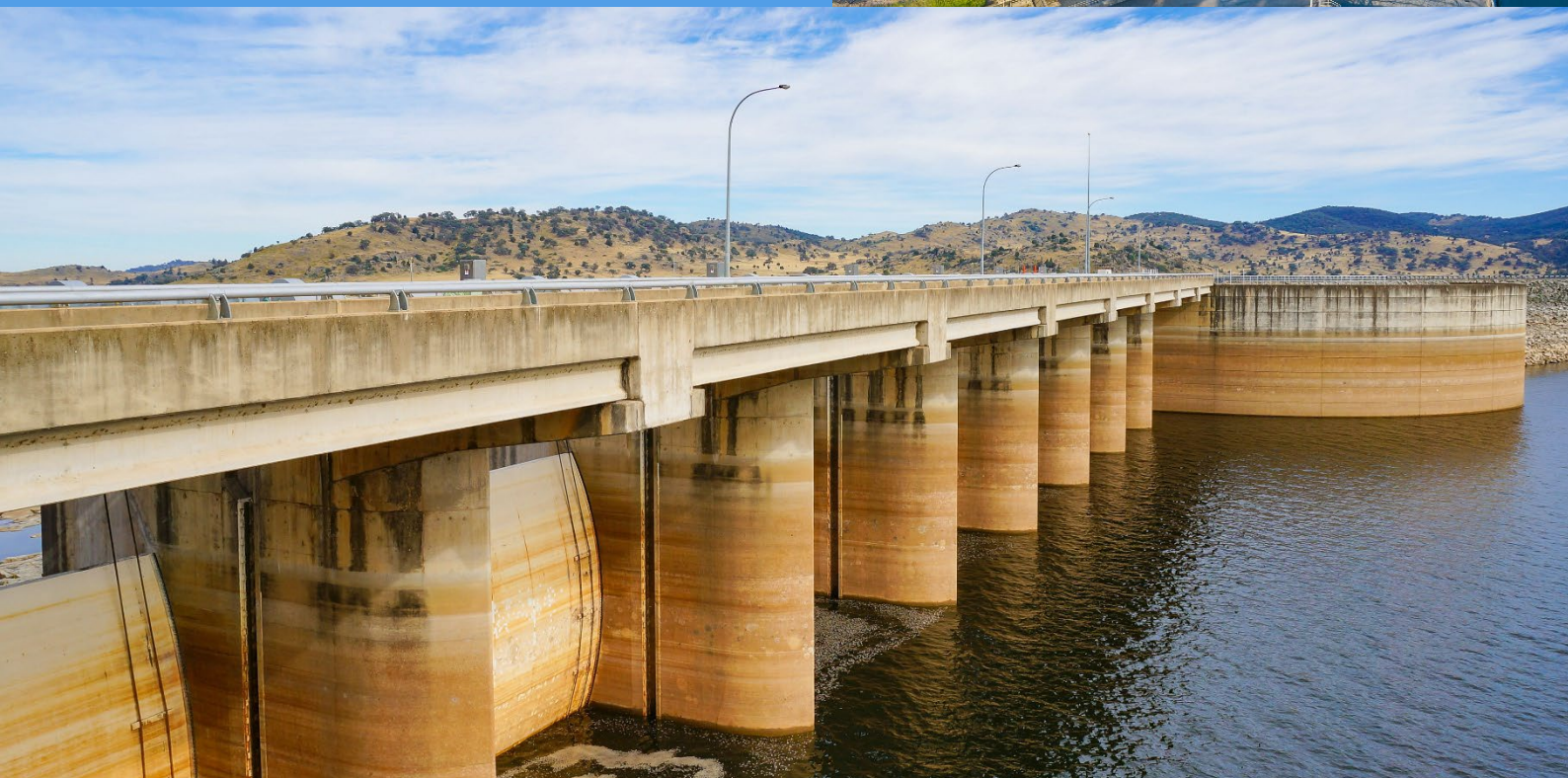
WATER SERVICES
ASSOCIATION OF AUSTRALIA

Submission to the Exposure Draft of the proposed enhancements to the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

May 2026



Submission to the Exposure Draft of the proposed enhancements to the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

Adam Lovell

Executive Director

Water Services Association of Australia

Level 6, 75 Elizabeth Street

Sydney NSW 2000

[redacted]

Luke Sawtell

Industry Co-Chair

Water and Sewerage Sector Group

[redacted]

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 on the Exposure Draft of the Critical Infrastructure Risk Management Program (CIRMP) Rules under the *Security of Critical Infrastructure Act 2018* (SOCI Act). As outlined in the sector's response to the consultation paper in February 2026, the water sector broadly supports measures to appropriately strengthen Australia's national resilience for higher-risk asset classes, including critical water assets. Water and wastewater services are essential to public health, community wellbeing and economic stability, and the sector recognises the importance of ensuring that national security risks are appropriately identified and managed.

The water sector has a strong and long-standing record of voluntarily acting on Government advice where that advice is specific; clearly linked to a credible threat; proportionate in cost and effort; and capable of being integrated into existing governance and risk management arrangements. This reflects the water sector's commitment to mature, risk-based decision-making and continuous improvement in resilience outcomes. Experience from past consultations has demonstrated that regulatory measures intended to formalise consideration of national security risk, will only achieve their intended purpose where the scope; evidentiary expectations; and lifecycle of such obligations are clearly defined with mechanisms to prevent cumulative or contradictory requirements. In the absence of such clarity, there is a risk that compliance obligations may drive administrative or box-ticking outcomes rather than genuine; risk-informed; collaborative security uplift.

The water sector acknowledges that the Exposure Draft reflects a genuine effort to respond to consultation feedback, including improved integration of national security considerations within the existing CIRMP material-risk construct and increased flexibility through revised transition arrangements. These changes represent progress toward a more principles-based and workable regulatory framework. Nevertheless, several issues remain unresolved, particularly in relation to unclear or undefined terminology; alignment with existing SOCI Act concepts; and funding for price-regulated water utilities.

This submission therefore recognises areas of improvement while highlighting matters requiring further refinement to ensure the CIRMP Rules remain proportionate, practicable, and aligned with the operational and regulatory realities of the water sector. The water sector remains committed to constructive engagement with Government to achieve regulatory outcomes that strengthen national resilience while safeguarding public health, service continuity and affordability.

ALL-HAZARD MEASURES

Consideration of specified risk advice

The revised changes to Section 6A provide industry with improved guidance on the management of national security risk within the existing CIRMP material-risk construct.

However, the water sector notes that the term *"impairment"* is not defined within the SOCI Act except in the context of electronic communications. The use of this term therefore introduces ambiguity, when applied more broadly to critical infrastructure risk. The sector recommends that the rules either include an appropriate definition of *impairment* or replace the term with the existing and well-understood SOCI Act concepts *relevant impact* or *significant impact*.

The sector also notes that Section 6A(b), which addresses Foreign Ownership, Control and Influence (FOCI) risk, is not directly linked to the existing definition of influence and control provided in Section 8A of the Act. Where intelligence reporting suggests that the nature of FOCI risk has evolved, consideration should be given to either amending the primary legislation or providing a clear explanation of the updated interpretation through Section 3 of the proposed rules, to ensure consistency and legal clarity.

CYBER AND INFORMATION SECURITY HAZARD MEASURES

Cyber security framework uplift

The sector appreciates the grant of an additional six months to transition to Security Level 2. However, the capacity of price-regulated water entities to achieve this uplift within the revised timeframe remains highly uncertain.

As outlined in the sector's February submission, medium-sized utilities (100,000–200,000 connections), operating in smaller states or regional contexts with well-developed IT and OT environments, can expect typical capital expenditure in the order of $15–20 million. Larger entities anticipate costs exceeding $120 million. While the Department of Home Affairs has engaged with the water sector's pricing regulators on the evolving threat environment, no regulator has indicated even in principle support for an expenditure of this magnitude.

Water utilities are regulated natural monopolies and, in most jurisdictions, operate under fixed three-to-five-year price determinations that set operating and capital allowances in advance, limiting the sector's capacity to absorb new material obligations outside established pricing cycles. With these constraints in mind, achievement of compliance by the 2028 attestation period will not be possible without deviating from the 'program of works' agreed with jurisdictional pricing regulators responsible for setting water utility prices. The independent regulators must be convinced that additional expenditure on national security risk mitigation is prudent, efficient, and necessary, rather than precautionary or speculative. Should the Federal Government fail to make this case effectively, implementation of the proposed rules will only result in regulatory duplication; misallocation of scarce recourses; under investment in new plant and technology; and ultimately a reduction in national water resilience. In the absence of approved additional funding, it is unlikely that the required uplift can be achieved within the proposed transition period.

This creates a demonstrable risk that responsible entities will be unable to demonstrate compliance where pricing regulators do not approve the necessary expenditure. As most water utilities are State and Territory owned, this misalignment between Commonwealth regulatory requirements and jurisdictional funding approvals introduces a risk of inter-government tension and implementation delay.

To address this risk, the sector recommends that the grace period be extended to a minimum of 36 months, with entities required to demonstrate planned and progressive steps toward achievement of Security Level 2.

The Department needs to clarify what it means by Level 2 and how it maps across maturity frameworks. The draft appears to reference Cybersecurity Capability Maturity Model (C2M2 i.e., Level 2 on a three-level scale). Many regulated entities use other maturity models (including five-level models such as Capability Maturity Model Integration (CMMI)). The Department should publish an explicit mapping or a recognition approach showing how common maturity models can be translated to the intended Level 2 threshold, including worked examples and evidence expectations for attestation to avoid inconsistent interpretation and unnecessary compliance effort.

Furthermore, Government has already indicated further regulatory reforms beyond those in the current Exposure Draft. Government needs to develop a long-term uplift strategy and regulatory roadmap, to provide industry with greater clarity on the regulatory expectations that lie ahead. For example, if the expectation is regulated entities meet maturity level 3 / 4 of the associated cyber framework within 5 / 7 years, this should be shared now. This would provide industry with certainty and better enable longer term funding strategies, in step with pricing regulators.

Critical systems network protection

Consistent with the issues identified for cyber framework uplift, the costs and complexity associated with network segmentation and resilience appear to be underestimated in the development of the proposed rules. While the sector welcomes the extension of the grace period, pricing regulators have not yet supported allocation of the additional funding necessary to implement these measures.

The rules introduce the concept of *critical systems* without providing a definition in the SOCI Act, the existing CIRMP Rules, or the proposed amendments. Given the centrality of this concept to compliance with the proposed obligations, a clear definition of what constitutes a responsible entity's

critical system(s) must be incorporated into either the primary legislation or the rules. The definition should include whether a tiering concept such as mission critical; business critical; or customer critical is intended, noting that regulated entities often apply internal criticality tiers differently and may identify a small subset of "most critical" systems within a broader criticality schema. Failure to clearly define critical systems risks misdirecting risk mitigation efforts and undermining regulatory effectiveness. The sector notes that the Independent Review of the *Security of Critical Infrastructure Act 2018* identified the need for clearer statutory guidance in this regard.

Phishing-resistant multi-factor authentication

Regarding rule 8A(5), the water sector remains concerned that no guidance is provided on what constitutes an appropriate phishing-resistant MFA standard. The absence of such guidance creates a risk that responsible entities may invest significantly in controls that are later deemed inadequate, requiring inefficient reinvestment.

The sector recommends that Government either publish guidance identifying MFA approaches that meet phishing-resistant expectations, or amend the rule to read:

> (*5) Subject to subsections (6) and (7), a responsible entity for a CI asset specified in subsection 4A(1) must establish and maintain a process or system in the entity's CIRMP to so far as is reasonably practicable to do so implement multi-factor authentication controls.*

Service continuity and resilience measures

The water sector is concerned that rule 8A(9)(b), which formalises the Australian Signals Directorate's CI-FORTIFY guidance and focuses on the restoration of IT and OT systems rather than the sustainment of critical services. These framing risks misdirecting resilience investment away from business continuity outcomes that may be more effective in maintaining essential services than recovery of disrupted IT and OT systems.

The sector suggests that the rule be re-drafted as follows:

> *(9)(b) ensuring that the responsible entity continues to provide an appropriate level of service for a period of three months while other networks are in a state of restoration and recovery.*

A similar concern applies to rule 8A(10)(b), which focuses on the critical asset rather than the continuation of critical services or functions. The sector recommends the rule be amended to:

> *(10) (b) (b) ensuring an appropriate level of service is maintained whilst rebuilding critical systems.*

We also suggest that the Department is more specific about service continuity and resilience expectations, it is unclear whether regulated entities need to be able to demonstrate they can operate for three months while disconnected from the internet, or something else.

PERSONNEL SECURITY HAZARD MEASURES

As noted in the sector's response to Critical systems network protection, the failure to provide a definition of what constitutes a critical system, limits the sector's capacity to assess the appropriateness of, and operational complexity in, complying with Section 9A.

The sector appreciates the Government's willingness to acknowledge that individuals who hold a AGSVA Negative Vetting 1 (NV1) clearance do not need to undergo an AusCheck clearance, however, the rules as written include three issues of concern:

1. The rule as written does not recognise individuals holding clearances above NV1 (NV2 and Positive Vetting).
2. The rule does not acknowledge the administrative arrangement where an individual moving between employers will have their active clearance suspended until the clearances is re-sponsored and the clearance reactivated.
3. There are no provisions in the current rules for recognition of a commensurate five-eyes clearance, despite such recognition being part of the AGSVA arrangements.

These issues create an unintended administrative burden, where a person with holding an appropriate clearance may, nevertheless, be obliged to undergo the AusCheck process due to poor drafting of the rules. There should also be greater certainty about acceptance of inactive clearances being allowed 'at the time the person was identified to be an onshore critical worker'.

In a highly competitive labour market, delays in AusCheck processing for key technical roles can have significant operational impacts; the sector therefore recommends that the Department clearly articulate expected AusCheck service levels (including target timeframes) to minimise implementation risk.

While captured in 8A of the Amendments, the need to background check offshore workers is problematic, without an accredited provider and adequacy advice. The Department should provide advice or endorse accredited providers to facilitate foreign worker background checks.

SUPPLY CHAIN MEASURES

Supply Chain mapping

The terminology used in the supply-chain mapping obligation is not aligned with commonly accepted resilience standards, creating potential confusion as industry seeks to align regulatory obligations with Australian and international benchmarks. The sector recommends that the term 'maximum tolerable outage' in section 10A(3)(b) be replaced with Maximum Tolerable Period of Disruption (MTPD) or Maximum Acceptable Outage (MAO) to align the measure with *ISO 22301 Business Continuity Management Systems*.

Vendor assessment

As noted in the water sector's response to the all-hazard measures proposals (see above), the absence of a definition of FOCI in the proposed rules risks inconsistent interpretation and mitigation across the sector. While the sector appreciates the Government's intention to retain a principles-based regulatory approach, leaving the identification of FOCI risk entirely to regulated entities increases the risk of resource misdirection and inadequate mitigation outcomes.

This risk is compounded by the Government's refusal to provide any form of vendor risk designation, effectively transferring all supply-chain integrity responsibility to regulated entities. This position is difficult to reconcile with examples cited during consultation, such as the Government's prohibition on DeepSeek AI, which illustrate circumstances where Government-led risk determination is both necessary and appropriate.

PHYSICAL SECURITY HAZARDS AND NATURAL HAZARDS

The sector supports the physical security requirements outlined in section 11A(1) as providing appropriate regulatory guidance for the identification and mitigation of physical security hazards. However, section 11A(2) is highly prescriptive, creates unreasonable regulatory burden, and is not commensurate with the physical security risk environment currently faced by the water sector.

Noting that additional physical security controls were not the subject of consultation, the sector recommends that section 11A(2) be removed from the rules and incorporated into best-practice guidance as a means of operationalising section 11A(1).

If section 11A(2) is retained, it should be amended to rrecognise performance against state and territory based protective security frameworks. For example, several of the requirements of 11A(2) are existing requirements of the South Australian Protective Security Framework (PSF).

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 Australian 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.

Adam Lovell

Executive Director

Water Services Association of Australia

Level 6, 75 Elizabeth Street

Sydney NSW 2000

[redacted]

Luke Sawtell

Industry Co-Chair

Water and Sewerage Sector Group

[redacted]