WATER SERVICES
ASSOCIATION OF AUSTRALIA

Water Services Association of Australia & Water and Sewerag

Submission to the proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

February 2026

Submission to the proposed amendments to enhance 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]

[redacted]

Luke Sawtell

Industry Co-Chair

Water and Sewerage Sector Group

[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 on the proposed amendments to enhance the Critical Infrastructure Risk Management Program (CIRMP) Rules. The sector broadly supports measures to appropriately strengthen national resilience for higher-risk asset classes, including critical water assets.

The sector has a strong 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 frameworks. However, the proposed specified risk advice measure will only achieve its intended outcome if the scope, evidentiary expectations, and lifecycle of such advice are clearly defined, including mechanisms to prevent cumulative or contradictory obligations. Without this clarity—particularly where advice is insufficiently detailed to support a meaningful risk assessment—the sector is concerned the measures may lead to a compliance focused, box ticking approach rather than a genuine risk-informed security uplift, despite the sector's demonstrated willingness to engage constructively.

In relation to foreign ownership, control and influence (FOCI) and vendors of concern, the sector notes that Australian water utilities are predominantly government-owned and operate within strong public health, operational assurance, and governance frameworks that limit direct exposure to inappropriate influence. The more significant challenge lies in indirect FOCI risks arising through complex commercial arrangements and multi-tier supply chains. Utilities have limited access to actionable, vendor-specific national security information and limited visibility beyond the sector's Tier 1[1] suppliers, yet the proposed changes will require entities to make defensible supply-chain decisions that must also satisfy jurisdictional procurement obligations and economic regulators. Without clearer Government provided risk determinations, directions, or practical guidance, the sector is concerned the proposed reforms may shift responsibility for opaque national security risk assessment from Government—where intelligence access and established mechanisms reside—to the water utilities.

Across the Consultation Paper's proposed cyber, supply chain, and personnel security uplifts, the sector's overriding constraint is funding the required security uplift within jurisdictional pricing determination periods. 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 may not be possible without deviating from the 'program of works' agreed with jurisdictional economic regulators responsible for setting water utility prices. The independent economic 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.

[1] Tier 1 suppliers provide goods and services directly to the water utility, primarily through a contractual relationship

All-Hazard Measures

All-hazard 1: Consideration of specified risk advice

Are there any controls on the scope of this measure that your organisation would suggest to assist with compliance and implementation?

The water sector supports the development of a rule that will oblige SOCI-regulated entities to consider the Government advice, identify whether it poses a material risk to the availability or function of their asset, and minimise or eliminate the material risks, as far as reasonably practicable. The sector has consistently demonstrated a willingness to voluntarily comply with Government advice, where that advice is: specific, clearly linked to a realistic and understood threat, and where compliance costs are proportionate to the risk.

The water sector's response to the PSPF Direction 001-2025, as well as its actions in response to Australian Signals Directorate threat and vulnerability advisories, illustrate this commitment. When such advice is provided, any failure by an organisation to properly consider it; assess its relevance and take appropriate action will have direct consequences, including: potential voiding of insurance coverage and reputational damage. The sector notes that a regulatory mechanism is not required to implement such arrangements but may add an additional significance to its consideration.

However, where the advice is general in nature, not attributed to a known threat actor, or cannot be meaningfully risk assessed, due to insufficient detail, industry is less able to make informed risk-based decisions. If obliged to do so through regulation, entities may be forced to adopt a bureaucratic, box-ticking, compliance-focused approach. It is the water sector's view that such approaches rarely achieve the desired outcome. When considering whether a regulatory measure is an appropriate vehicle for delivering this requirement, the sector is concerned that Government has not fully considered the existing level of voluntary compliance within the water sector.

The proposed measure fails to identify which sources of risk advice would need to be considered, nor how an entity would demonstrate compliance. For example, if a water sector entity assesses that certain advice does not present a material risk to its operations, must that assessment form part of its CIRMP for the life of the program? Or is it sufficient to make the decision through the entities risk management processes? The sector recommends that the rule include provisions that clearly distinguishes between general risk-advice and best practice information, and the specific advice which must be considered. In developing the rule, the Department must also consider the impact of its audit and compliance program and if those findings and/or advice would also create regulatory obligations.

The sector notes the proposed rule places no obligation on the Government to consider the ongoing relevance or appropriateness of its advice. Nor is the Government obliged to consider how individual pieces of advice interact with other risk mitigation measures and existing controls.

Given the dynamic nature of the security threat environment, and the highly regulated nature of the water sector (in addition to critical infrastructure obligations, water utilities are subject to economic, public health, environment, competition, health and safety and other corporate regulatory frameworks), there is a demonstrable risk that compounding and contradictory compliance obligations may accumulate over time; unless a mechanism for regular review, consolidation and, where appropriate, withdrawal of advice accompanies the proposed rule. The sector suggests that the Gov Team's hosted TISN platform provides an appropriate forum for hosting both general risk advice and enforceable obligations[2].

[2] Noting that these must also be promulgated on the Federal Register of Legislation.

Could existing engagement mechanisms be adapted or improved to deliver more value, and support this obligation?

The water sector recommends that the Government develop annual sectoral risk advice in which individual threat and risk information is reviewed, consolidated and presented against a holistic assessment of the current security environment. Such an approach would simplify the sector's compliance obligations and reduce the need for organisations to respond to an ever-growing list of regulatory obligations. To be effective, publication of this annual advice should be timed to allow entities sufficient opportunity to incorporate it into their SOCI compliance and attestation processes—ideally six months before the end of the financial year.

The advice should consolidate all relevant regulatory guidance issued in the preceding 12 months and clearly identify any changes, including the formal withdrawal of superseded, inappropriate or outdated advice. This would provide greater clarity for industry and reduce the risk of conflicting or duplicative obligations.

The water sector also considers it appropriate for individual organisations to retain the right to determine whether the advice presents a material risk to their operations and to respond accordingly. For this measure to function as intended, Government should not require entities—through attestation or compliance processes—to demonstrate that specific mitigation actions have been implemented. Such an approach would undermine organisations' ability to manage risks through their established governance frameworks and could inadvertently convert flexible, risk-based advice into prescriptive regulatory requirements.

All-hazard 2: All-hazard material risks - foreign ownership, control and influence

Are there other specific material risks, like those arising from FOCI, that your organisation minimises or eliminates in their CIRMP?

While governance and leadership arrangements vary across entities, the Australian water sector is predominantly composed of government-owned utilities that operate within their jurisdictional policy and regulatory frameworks. These ownership structures have historically limited the sector's direct exposure to FOCI risks. Consequently, the sector does not support implementation of this measure as it unnecessary for our sector.

As part of its overarching responsibility to deliver a safe; secure; and reliable water supply, the sector has established mature and comprehensive risk management arrangements designed to address a broad spectrum of potential threats. Although the content of a CIRMP will reflect an individual entity's assessment of its operational and regulatory environment; the core obligation to maintain the safety and integrity of the water supply ensures that all utilities remain focused on identifying, managing and eliminating risks that could compromise service quality or public health. These mitigation arrangements include mechanisms that independently validate water quality through multibarrier controls, independent water quality monitoring and testing, and customer feedback processes. Water utilities also operate within strong governance and reporting frameworks, providing regular assurance to their boards, government owners and regulators. Management arrangements are designed to mitigate a broad spectrum of potential threats. Water utilities also operate within strong governance and reporting frameworks, providing regular assurance to their boards, government owners and regulators.

These layers of control and oversight demonstrably reduce the capacity of a hostile state actor to use FOCI to directly impact water and wastewater operations and their capacity of FOCI to undermine the sector's resilience. If an entity was to become aware (through formal or informal channels) that a foreign actor was attempting to inappropriately influence its operations, existing risk management and governance mechanisms exist to empower the entity to implement appropriate mitigation measures quickly and escalate the matter as necessary. Nevertheless, the sector acknowledges that mitigation FOIC risk is a wicked problem, with attempts to

exercise control and influence being deniable; opaque; and/or covert. For these reasons the sector supports an enhance exchange of FOCI information between the Federal and jurisdictional government (including with local government) so that they can make and support appropriate risk-based decisions when acting as the utilities owners. This should be accompanied by regular information exchanges with economic regulators so that they can appropriately assess the appropriateness of measures taken by the sector to mitigate FOCI risks.

Of more relevant concern is the potential for indirect third-party FOCI risks to be introduced through commercial arrangements including joint-venture investment and supply chains. Given the opaque nature of this threat, the sector is highly reliant on Government advice. While an awareness of potential threats is useful (for example the potential impact of the 2017 Chinese National Intelligence Law on Chinese commercial entities) it provides an inadequate basis for an entity to implement appropriate risk management decision. To appropriately make such decisions, industry requires clear and unambiguous advice from Government on risks to avoid (for example the Deep Seek AI advice) or advice on appropriate risk-mitigation measures to counter potential FOCI risks. If provided with this advice, water entities will act in accordance.

In considering this measure the sector makes the following observations:

- The Foreign Investment Review Board (FIRB) already has established processes for the consideration of FOCI risk and can make such assessments for CI at the zero-dollar framework. Given the intelligence and information gathering resources available to Government and the FIRB, the sector believes that ownership and control risks can be appropriately managed through those mechanisms. This could be strengthened through empowering the FIRB to retrospectively re-consider its risk assessment. However, such a measure must be carefully balanced against sovereign risk considerations.
- For government-owned water sector entities the rule ignores the entities' obligations to comply with jurisdictional investment and procurement rules. If FOCI risks are not clearly described by the Federal Government, the entity may not be able to comply with its procurement obligations, potentially creating a regulatory conflict.
- The sector notes that the Federal Government has been unwilling to create either a register of either low or high FOCI risks suppliers and product. Consequently, the proposed obligation will transfer FOCI risk from the Federal Government to the water sector, despite the Government's greater access to FOCI information. Creation of either a trusted supplier list or a do not use list would significantly enhance the sector's capacity to make FOCI-informed risk management decisions.

Does your organisation currently consider FOCI risks in their CIRMP?

This question is most appropriately answered by individual entities.

Regulatory Impact Analysis

Given the lack of detail provide regarding the type and frequency of advice and direction that may be offered under these rules, it is impossible to provide meaningful advice on the regulatory impact of the proposed risk advice and FOCI proposals. Nevertheless, the water sector provides the following advice for consideration.

- The water sector operates under economic and pricing regulation, with costs fully recovered from customers, meaning any increase in operating costs flows directly to customers through higher water and wastewater bills. Jurisdictional independent economic regulators are empowered to set water prices for each regulatory period (three to five years depending on jurisdiction). Consequently, water sector entities have very limited capacity to independently resource high-cost risk mitigation measures.

- There is a tension between the Federal Government's policy objective of seeking an increase in critical infrastructure security, with additional obligations imposed on the higher-risk sectors. Jurisdictional government policy which seeks to deliver reliable water and waste water services to the community, while obtaining an economic return on investment as the owner of the water utility and minimising costs to the consumer. As mitigation of FOCI risks, particularly FOCI risk in supply chains, will typically increase the sector's capital and operating costs, the sector believes the Federal Government must take responsibly for the additional security and resilience costs that will ultimately be imposed on the community.

- Water utilities routinely invest to manage risks as they arise, and currently there is increased investment across many water utilities to deliver essential infrastructure for new housing (a national policy objective). New requirements, such as the changes proposed to the CIRMP Rules, add to the investment pressures. Without a commensurate increase in revenue, these additional pressures will divert investment away from essential infrastructure for housing and represent an unnecessary regulatory burden that reduces productivity and is counter to Federal and jurisdictional governments' policy objectives.

  The sector's experience has been that the economic regulators will not approve price increases and/or pass-through measures to customers without a rigorous cost-benefit analysis, that demonstrates the measures are prudent; efficient; and necessary. The ad-hoc and truncated approach to assessing the regulatory impact of the proposed rules, suggests that the Department lacks the analytical capability necessary to satisfy that assessment threshold. Consequently, economic regulators are unlikely to accept the Department's costings as a basis for price increases and compliance with the measures will be unfunded. This will undermine achievement the policy objective and will reduce water-sector resilience.

- Government threat and risk advice is rarely provided with a sufficient level of specificity, sufficient for either the sector or our economic regulators to make meaningful judgment about the appropriateness of the measure and the potential impact on an individual customer's bill. This contrasts with industry which can and does cost such measures to an individual level. The sector observes that a greater understanding of the potential impact of its regulatory actions on individual consumers would greatly assist the Department in making appropriate cost and risk-informed decisions.

- The potential compliance costs for these measures will significantly impact utilities with smaller resource bases and larger geographic areas. In addition, imposition of these measures on entities that have been declared under Section 51 (less than 100,000 connections) would have a disproportionate impact on their financial position.

Cyber and Information Security Hazard measures

Cyber 1: Cyber security framework uplift

Where applicable, what maturity/profile does your organisation seek to achieve?

The water sector broadly supports an uplift in cyber security, but the sector believes that the proposed 18-month transition period is unachievable due to the level of required investment and the timelines for independent economic regulators to make pricing determinations.

Water sector entities have selected cyber security frameworks that best align with their own business operations and cyber security arrangements. While individual maturity levels vary, based on their individual network design; resources; and geographical distribution, most entities have achieved or seek to achieve Level 1 maturity, with higher security settings generally applied to more important or sensitive system and applications. During FY 2024/25 the combined cyber security operating cost of 25 Australian water utilities[3] was approximately $59 million. Representing an average cost of cyber security on an Australian household's water bill of $6.09 per year.

Within this funding envelop, entities have also developed and/or implemented cyber security improvement plans to address their threat environment and potential vulnerabilities. This is combined with a funding strategy aligned to their regulator-approved pricing determinations. The sector notes that imposition of additional obligations outside of this pricing period will be unfunded, with costs diverted from other projects. Typically, capital investments to support housing growth, renewal of infrastructure and network resilience programs.

In considering the proposal uplift to Level 2, the sector provides the following advice:

- For most entities, achieving organisational-wide Level 2 compliance will require significant multi-year investment.
    - For smaller regional entities (<100,000 connections) an investment of $1-$15 million dollars to upgrade hardware and software may be required. For these entities, access to suitably qualified ICT and cyber security personnel is highly challenging with the limited number of available professionals expecting to be renumerated at rates commensurate with metropolitan counterparts. While some work can be undertaken remotely for corporate systems and network this is not practical for the maintenance of water sector Operational Technology (OT).
    - For medium-sized utilities (100,000-200,000 connections) based in either smaller states or within regions, with well-developed; maintained and managed Information Technology (IT) and OT architecture, an estimated capital expenditure of $15-$20 million is typical.
    - For larger entities servicing widely dispersed areas or capital city environments (>200,000 connections) with large asset bases, the predicted transition costs may exceed $120 million.
- For all entities, the regulators' approved level of cyber security funding is unlikely to deliver the desired level of whole-of-business cyber security uplift within the Department's proposed 18-month transition period. Although the total costs will depend on an individual utilities' size, customer base, and geographic coverage, the following considerations are common across the sector:
    - Australian water and wastewater treatment assets are ageing and require ongoing maintenance with little redundancy available for systems designed to provide

[3] Representing over 90% of the Australian water and sewerage services sector revenue and more than 80% of connected properties.

continuous operation. Changes must be carefully planned and aligned with plant and asset maintenance cycles, otherwise supply disruptions and/or public health risks are highly likely to occur.

- The water sector's economic and pricing regulation combined with 50+ year asset management lifecycles limit the sector's capacity to rapidly acquire and deploy new IT and OT into operational water and wastewater networks. Due to regulatory requirements; planning obligations; licence conditions; limited numbers of trained OT personnel; acquisition timeframes and long-duration construction timeframes, the introduction of new IT and OT into existing infrastructure is highly complex and may not be practically achievable for entities within the proposed 18-month transition period.
- The Level 2 certification and assurance requirements are unclear. While a level of assurance will be necessary, the national OT audit and compliance capabilities will be challenged by the number of entities and the geographic distribution of the water and wastewater networks. Consequently, entities may be unable to demonstrably comply with the measures. The sector notes that not all the approved cyber security frameworks have Level 2 maturity levels, and the requirements to meet Level 2 across the frameworks are not consistent. These differences making comparison of security across the water sector and CI enterprise complex, resulting in inconsistent cyber security outcomes.
- For entities using a framework that does not include maturity levels, the introduction of a maturity overlay effectively introduces a second framework obligation, which was not a consideration when entities were determining which framework to apply when the Rules introduced this requirement. Many entities have already invested significantly in a framework that does not include maturity levels (e.g. ISO27001). The sector recommends that as the Department considers that a particular maturity level is important, then must explicitly specify the equivalent maturity framework for each framework listed in the rules, or assess and prepare a maturity framework with equivalent levels for all frameworks listed in the rules. This will provide clarity and all higher-risk sectors achieve a commensurate cyber security standard.
- The water sector is concerned about the rate of change within the cyber security regulatory environment. While a deterioration in the international security environment is acknowledged, the sector is concerned that the proposed regulatory changes are reactions to events; rather than a result of forward-looking and holistic threat assessments. Given the potential scale of investment required to comply with the proposed measures the sector would seek assurance that the obligations will not require a further uplift once Level 2 has been achieved.

For these reasons the water sector recommends a five-year transition period with a balancing obligation for entities to demonstrate planned enhancement to the IT and OT security levels during the transition period. We strongly recommend segmenting the obligations, so the Level 2 security level is applied only to an entities' most critical systems. Rather than a one-size fits all, whole-of-business requirement for achievement of Level 2. The water sector would also seek the Government's advice on medium-term (5-10 years) objectives to address emerging threats and emergent technologies.

How does your organisation invest in security beyond achieving minimum cyber framework compliance?

The water sector invests in security well beyond minimum cyber framework compliance through adoption of a risk-informed and operationally focused approach to protecting both IT and OT environments. The water sector has progressively hardened networks, with many utilities implementing controls that materially exceed the baseline requirements of their chosen cyber

security framework. These enhanced controls are prioritised around the most critical systems and processes, ensuring protection where the potential safety, health, or service consequences are highest.

Cyber security controls are further strengthened by the sector's multi-barrier safety and quality controls. With physical testing, operational monitoring, sampling regimes, and automated alarms collectively used to provide strong protection against unauthorised interference. Although these controls are primarily designed for safety and water quality assurance, they also function as highly effective all-hazards defences. Any covert manipulation of water quality; volume; or chemical dosing, triggers rapid detection and response due to the tight operational tolerances within the network. One distinguishing feature of water infrastructure, compared with other critical infrastructure such as electricity and communications, is the additional response time afforded by systems that fail open by design, reducing the potential for abrupt service loss.

The water sector's cyber security investment strategies are guided by a deep understanding of the operational environment and an ongoing assessment of risk, needs, and available resourcing. Each entity sets its own cyber security aspiration, expressed in part as a maturity target, based on an evaluation of the potential harm and its risk tolerances (zero for public health risk and typically very low for long-duration service disruptions). This tailored, risk-driven calculus is where regulatory scrutiny should focus, rather than on compliance with a uniform uplift obligation that may not reflect the sector's operational realities. In practice, this means the sector's cyber security investments are planned through a risk-informed decision-making approach that aligns protection levels with potential consequences. This ensures that IT and OT networks are secured to a level that is proportionate, defensible, and directly tied to the operational risks of the water sector.

Does your organisation face challenges in obtaining the necessary investment in security to reach compliance, or (where necessary) go beyond the minimum cyber framework?

As natural monopolies, water entities are subject to three-to-five price determinations by independent economic regulation. In setting the prices, regulators will seek to balance the utilities' need to maintain and develop their networks without adversely impacting on customers. Consequently, the funding of additional cyber security controls beyond regulated minimum standards and additional measures to protect public health and supply obligation, must be incorporated into the sector's regulatory approved funding arrangements.

The sector's independent economic regulators must be convinced that additional expenditure on national security risk mitigation is prudent, efficient, and necessary, rather than precautionary or speculative. Independent economic regulators have publicly expressed concerns about the potential for the increased security obligations to be used as a justification for inappropriate 'gold plating' of the sector's networks, with additional costs passed onto customers.

Cyber 2: Critical systems network protection

What current measures does your organisation implement to segregate critical systems from all other internet facing and less secure systems?

Most Australian water utilities have implemented a baseline level of segregation between IT and OT environments, with some treatment plants retaining limited capability to operate locally (often described as 'island mode') for a short period of time where necessary to maintain safe operations during loss of external connectivity.

However, segmentation within OT environments is materially more complex. OT networks have historically been engineered to maximise availability, continuity of supply, and operational resilience through interconnected architectures and shared services. As a result, internal OT

segmentation is frequently constrained by legacy designs, operational dependencies, and vendor/asset lifecycle considerations.

For smaller utilities operating a limited number of discrete plants or assets, it may be feasible to operate networks independently for a period, particularly where assets are not physically or operationally interconnected (for example, systems serving discrete townships or districts). However, operating under these arrangements increase public health, operational and regulatory risk.

For medium sized and larger utilities, existing OT network designs have generally prioritised reliability and redundancy rather than cyber resilience ‘by design’. Implementing deeper segmentation typically requires an architectural redesign aligned to recognised industrial security approaches, including establishing controlled intermediary services and restricting conduits between zones to explicitly authorised traffic only. Such changes cannot be introduced into live operational networks without operational risk. Accordingly, implementation must be staged and coordinated with plant isolation, planned outages, and commissioning windows. sized and larger utilities, existing OT network designs have generally prioritised reliability and redundancy rather than cyber resilience. For medium-sized and larger utilities, existing OT network designs have generally prioritised reliability and redundancy rather than cyber-resilience.

Indicative costs (medium sized utility approximately 100,000–200,000 connections)-sized utility

While precise costs are highly dependent on current architecture and the target security state, indicative order of magnitude costs for a medium sized utility are estimated as follows: --magnitude costs for a-sized utility

1. Baseline uplift – IT/OT boundary segregation (establishment of a secure, controlled intermediary network that sits between the corporate IT environment and the OT environments, with controlled remote access): $2–$5 million.

   This scope typically includes establishment or uplift of an intermediary environment between IT and OT hardened remote access via approved intermediaries (jump hosts/bastions), centralised logging/monitoring integration, and implementation of deny by default/allow by exception connectivity rules between IT and OT.

2. Targeted internal OT segmentation – treatment plants + most critical OT zones: $3–$10 million (additional to baseline).

   This scope typically includes OT network redesign at plants plus segmentation of high criticality systems (engineering workstations, SCADA servers, historians, safety relevant process networks) to reduce lateral movement risk. The design intent aligns to recognised practices for segmenting industrial environments into smaller trust zones. criticality systems (engineering workstations, SCADA servers, historians, safety relevant process networks) to reduce lateral movement risk. The design intent aligns to recognised practices for segmenting industrial environments into smaller trust zones. -criticality systems (engineering workstations, SCADA servers, historians, safety-relevant process networks) to reduce lateral movement risk. The design intent aligns to recognised practices for segmenting industrial environments into smaller trust zones.

3. Remote site segmentation– selective and risk based: $1–$6 million (additional to baseline, depending on feasibility).

   For remote assets the scope and cost will vary widely based on communications networks, physical constraints, and existing field networking capability. In many cases, segmentation is implemented pragmatically through hardened site routers/switches, constrained conduits back to OT operations, and standardised configurations.

Total indicative range (multi-year program): $5–$15 million. These costs will increase significantly for entities covering larger geographic areas, multiple treatment plants, and higher numbers of connections.

Does your organisation mandate security awareness training for users with access to critical systems?

Best answered by individual entities.

What measures does your organisation undertake to log who has access and can make changes to your critical systems?

Best answered by individual entities.

Does your organisation undertake logging and monitoring of network traffic?

Best answered by individual entities.

Cyber 3: Multi-factor authentication (MFA)

What type of systems in your organisation are currently protected by MFA?

The water sector supports implementation of MFA to protect IT and OT systems with SOCI regulated water entities have largely implemented MFA across corporate and cloud IT environments and for newly deployed or materially upgraded applications, particularly for remote access, privileged accounts, and cloud services.

For medium-sized water utilities servicing 100,000–200,000 connections, these controls are generally well established within enterprise IT and have materially reduced the risk of credential-based compromise in business systems. However, extending these controls to phishing-resistant MFA across all access pathways represents a significantly more complex challenge in the water sector.

The complexity is compounded by the absence of a government provided phishing resistant MFA standard or reference architecture to design against. Without clear guidance on approved authentication methods, assurance levels, applicability by use case, and minimum evidence requirements, utilities must independently interpret what constitutes phishing resistant MFA in practice. This results in bespoke solution designs, increased procurement complexity, inconsistent vendor capability, and higher costs associated with architecture development, integration, testing, and regulatory assurance. The lack of a prescribed baseline also makes it more difficult to demonstrate consistency with sector-wide expectations. This results in bespoke solution design-wide expectations, increasing organisational risk and uncertainty.

OT environments are often excluded from initial phishing resistant MFA implementations, or adopted later, due to practical technical and operational constraints. Many operational systems use legacy platforms, shared or noninteractive accounts, or vendor managed access arrangements that do not easily support modern phishing resistant authentication without significant changes. Introducing MFA in these environments can also create availability or safety risks if authentication issues delay operational response. As a result, utilities generally prioritise phishing resistant MFA for corporate IT and remote access first, while taking a staged, risk-based approach to extending controls to operational and vendor access as systems are upgraded.

For a medium-sized water utility (100,000–200,000 connections), the indicative cost of implementing phishing resistant MFA as a staged, multiyear program is typically in the order of $3–$12 million, depending on current maturity and the extent to which operational and third-party access is included. As a guide, this may include:

- $0.5–$2.0 million to uplift enterprise identity, remote access, and supporting controls to phishing resistant standards-resistant standards

- $1–$4 million to strengthen privileged access management so MFA is effective in practice
- $1.5–$6 million to redesign and control vendor and operational access pathways (including secure intermediaries, monitoring, commissioning, and changes to support models).

Costs are typically higher where legacy systems predominate and where implementation must be coordinated with constrained operational windows.

Are there system or/circumstances in which MFA is not reasonably practicable to use? If so, what other compensating controls are, or could be implemented?.

Many operational systems use legacy platforms, shared or noninteractive accounts, or vendor managed access arrangements that do not readily support modern phishing resistant authentication without significant system modification or changes to support models. Introducing MFA in these environments can also create availability or safety risks if authentication issues delay operational response. interactive accounts, or vendor managed access arrangements that do not readily support modern phishing resistant authentication without significant system modification or changes to support models. Introducing MFA in these environments can also create availability or safety risks if authentication issues delay operational response.

These challenges are compounded by the complexity of designing, procuring, and funding such uplifts within compressed timeframes, particularly where utilities operate under fixed five-year pricing determinations that did not anticipate the scope or cost of phishing resistant MFA.

Supply Chain Hazard measures

Supply Chain 1: Supply chain vulnerability mapping

To what level of upstream and downstream detail does your organisation currently map their supply chain?

While a level of supply chain mapping is an appropriate risk management practice, supply chain mapping in the water sector is inherently complex due to the scale, diversity, and longevity of assets and services required to deliver safe and secure drinking water and wastewater services.

Water utilities rely on a broad ecosystem of suppliers across construction, chemicals, mechanical and electrical equipment, OT, IT, maintenance, and specialist services. Many of these supply chains extend across multiple tiers and jurisdictions, making it difficult to identify downstream dependencies, concentration risks, and vulnerabilities beyond Tier 1 suppliers. This complexity is further compounded by long asset lifecycles (typically 50+ years) and legacy technologies, where original vendors may no longer exist and embedded components or subcontractors are not readily visible.

While comprehensive multitier mapping remains challenging, water utilities do undertake targeted and proportionate supply chain mapping for Tier 1[4] suppliers, particularly where those suppliers support critical operations or essential services. This typically includes maintaining an inventory of key Tier 1 suppliers, assessing their criticality based on service dependency, availability of alternatives, and potential operational or safety impacts, and undertaking enhanced due diligence where suppliers are assessed as high risk or high criticality. Such activities may include contractual reviews, assessment of financial viability, and collection of information on business continuity and disaster recovery arrangements, including reliance on sole source inputs or critical subcontractors.

Procurement and contract management processes are the primary mechanisms through which utilities maintain Tier 1 supply chain visibility. This includes embedding requirements for incident notification, change management, and continuity planning, supported by ongoing supplier

[4] Tier 1 suppliers provide goods and services directly to the water utility, primarily through a contractual relationship.

engagement and performance monitoring. These activities provide a practical and defensible level of visibility over the most immediate and controllable supply chain risks; however, visibility typically diminishes beyond the first tier due to limited contractual leverage and information availability. As a result, supply chain mapping in the water sector is generally treated as an ongoing, risk-based activity that supports operational resilience, rather than a comprehensive end-to-end mapping of all upstream dependencies.

Does your organisation keep a list or record of alterative approved suppliers?

Water utilities seek to maintain records of approved alternative Tier 1 suppliers for critical goods and services where this is reasonably practicable, and use procurement and contract management processes to identify, assess, and manage Tier 1 supply chain risks as part of broader risk management arrangements. This approach aligns with SOCI expectations that responsible entities identify material risks and so far, as is reasonably practicable, take steps to minimise or eliminate those risks, including risks arising from supply chain hazards.

However, water utilities recognise that the Australian water chemicals market is relatively concentrated, with a limited number of national suppliers and regional distributors providing critical treatment chemicals and often relying on shared manufacturing capacity, imported feedstocks, and common logistics pathways. This concentration can constrain the availability of genuinely viable alternatives, particularly where substitution is limited by regulatory approvals, product compatibility, or storage and delivery constraints. Accordingly, water utilities apply a risk-based interpretation of ‘reasonable steps’, maintaining alternative supplier options where feasible and supplementing this with contingency measures—such as stockholding strategies (where possible to do so given the safety and quality risks associated with chemical stockpiles), prioritisation arrangements, and proactive supplier engagement, where alternative sourcing is not practicable

Does your organisation have real-time access to data surrounding supplier availability?

Best answered by individual entities.

Supply Chain 2: Vendors of concern

How does your organisation currently map vendors of concern in your supply chain?

Water utilities will, seek to map vendors of concern through a risk based, Tier 1 (direct supplier) approach embedded within procurement, and contract management. This focuses on suppliers that support the delivery of essential water and wastewater services, including treatment chemicals, OT, IT systems, construction and maintenance services, and specialist operational support. Tier 1 suppliers are identified and assessed based on criticality to service continuity, access to critical systems or sites, concentration or sole supplier risk, and known ownership or control considerations where information is available. Tier 1 (direct supplier) approach supplier-supplier risk, and known ownership or control considerations, where information is available.

Vendor of concern identification is informed by a combination of supplier disclosures, contractual information, publicly available data, and internal risk assessments rather than classified national security intelligence, which is not routinely accessible to water utilities. This limits the ability to make definitive judgements about national security related concerns and requires utilities to rely on indicators such as service criticality, access privileges, cyber and operational assurance posture, and dependency risks. As a result, concern is assessed pragmatically in terms of potential operational, safety, and service delivery impacts rather than intelligence led threat attribution.

Visibility typically diminishes beyond Tier 1 suppliers. Many critical water sector inputs, particularly chemical; equipment; and OT components, rely on complex and often overseas

manufacturing and logistics chains, limiting transparency over Tier 2 and Tier 3 suppliers. Water utilities generally lack contractual leverage to compel detailed disclosure of upstream suppliers and subcomponents and therefore prioritise mapping and assurance activities where they are most effective and reasonably practicable, at the direct supplier level, while applying compensating controls such as stockholding, redundancy, and contingency planning to manage risks associated with Tier 2 and 3 suppliers.

The water sector's supply chain risk mapping capability is also shaped by Australian competition and laws, and jurisdictional procurement obligations. This constrains the extent to which water utilities can share commercially sensitive supplier information or collaborate directly with peers to collectively identify vendors of concern.

What current security measures are put in place if a vendor of concern is identified?

Best answered by individual entities.

Does the wider government provide adequate material to support you to identify a vendor of concern and mitigate their potential impact?

The water sector considers that the Government does not currently provide sufficient or sufficiently specific material to fully support the identification of a vendor of concern or to enable defensible mitigation decisions at the level of detail expected by economic regulators responsible for setting water utility prices.

While Government guidance establishes high-level expectations under frameworks such as SOCI and CIRMP, requiring entities to identify and manage supply chain risks so far as is reasonably practicable, it does not provide industry or economic regulators access to detailed, vendor specific national security information or actionable intelligence that would allow water utilities to confidently assess concern beyond publicly available information and supplier disclosures.

In practice, water utilities do not have access to classified or sensitive national security assessments relating to specific vendors, ownership structures, foreign influence, or upstream supply chain risks. This limits the ability to make objective, evidence-based determinations that a vendor constitutes a national security concern, particularly where the vendor is widely used across the sector or operates lawfully within Australia. As a result, utilities must rely on indirect indicators (such as service criticality, concentration risk, access privileges, and contractual controls) rather than authoritative threat information when assessing and mitigating vendor risk.

This information asymmetry creates a material challenge when responding to pricing and economic regulators, who may reasonably seek clear justification for decisions that increase costs, restrict supplier choice, or require capital investment to mitigate vendor risk. Without access to Government provided, vendor specific security assessments or a clear mechanism for reliance on Government determinations, water utilities are exposed to regulatory risk when attempting to demonstrate that mitigation actions are prudent, efficient, and necessary, rather than precautionary or speculative. Accordingly, while water utilities take reasonable and proportionate steps within their control to manage supply chain risk, the absence of detailed and shareable Government security information constrains the ability to both identify vendors of concern with confidence and to evidence mitigation decisions in a manner that fully addresses the expectations of economic regulators.

Are there other options to reduce the FOCI risk posed by vendors of concern, either in addition to or instead of the proposed approach?

The water sector considers that supply chain resilience could be materially strengthened through more structured and trusted exchange of vendor risk information, both within the water sector and across other critical infrastructure sectors that rely on common suppliers, technologies, and service providers.

Many critical vendors in: OT; IT; construction services; and treatment chemicals, operate across multiple utilities and sectors, meaning that risks related to concentration, vendor failure, or security concerns are often systemic rather than entity specific. Greater information sharing would support earlier identification of emerging risks, reduce duplication of due diligence effort, and enable more coordinated and proportionate mitigation responses.

However, the ability to share vendor risk information is significantly constrained by Australian competition law, including the absence of a clear and general statutory defence or safe harbour mechanism within the primary SOCI legislation for good faith information sharing undertaken for national security or critical infrastructure resilience purposes. In the absence of explicit protections, water utilities must be cautious about sharing information that could be interpreted as commercially sensitive; influencing supplier choice; pricing; or market behaviour, even where the intent is risk management rather than collusion. This creates a chilling effect on collaboration and results in largely siloed assessments of vendors that are known to be common across the sector.

As a result, current information exchange tends to be informal, limited in scope, or confined to high-level engagement through Government led forums, rather than systematic sharing of actionable vendor risk insights. The water sector considers that clearer legislative or regulatory mechanisms such as an explicit SOCI information sharing safe harbour; government facilitated intelligence sharing; or regulator endorsed sector coordination arrangements, would materially improve supply chain risk management while maintaining appropriate safeguards against collusion or anticompetitive behaviour.

Regulatory Impact Analysis

In 2024/25, WSAA analysis of 25 Australian water utilities indicated combined chemical expenditure of $149.6 million for water (network and treatment) and $102.8 million for wastewater (network and treatment), totalling $252.4 million. This chemical spend represents approximately 1.5% of revenue from water and sewerage services and 3.43% of total operating costs, highlighting that while chemicals are a relatively small share of revenue, they are a material and unavoidable component of operating expenditure.

Over the three years from 2021/22 to 2024/25, the 12 largest Australian water utilities experienced a 22% real increase in chemical costs, demonstrating that chemical inputs are already subject to sustained cost escalation and supply volatility.

Supply chain risk mitigation measures, such as avoiding higher-risk vendors or geographies (for example, not sourcing critical components from China); increasing supplier assurance requirements; or shifting to alternative sources, are likely to impose a premium on chemical procurement.

Using the 2024/25 chemical spend of $252.4 million as the baseline, a uniform uplift of 5–30% would imply additional annual costs of approximately $12.6 million (5%), $25.2 million (10%), $37.9 million (15%), $50.5 million (20%), and $75.7 million (30%) across the 25 utilities. Expressed as sector impacts, these increments equate to approximately 0.075–0.450% of revenue and 0.171–1.029% of operating costs, which is material in the context of efficiency expectations and constrained operating expenditure allowances, and ultimately impacting customer bills.

The water sector's annual chemical spend of $252.4 million equates to approximately $21.0 million per month; therefore, holding an additional one to three months of inventory to improve resilience implies $21–$63 million in additional working capital tied up in inventory (with associated carrying, storage, handling, and obsolescence risks). Accordingly, when assessing prudency and efficiency, chemical supply chain risk mitigation should be treated as a multi-factor cost driver (price premium + resilience measures).

In addition to unit price impacts, supply chain risk mitigation frequently requires non-price measures that introduce further cost pressures, including: increased stockholding to manage longer lead times or reduced supplier redundancy; supplier qualification; re-approval activities; and enhanced quality assurance, with a material impact on operational expenditure.

Personnel Security Hazard measures

Personnel 1: Personnel security plan

Personnel 2: Strengthened background checking

Personnel 3: Enhancing personnel material risks

The water sector broadly supports the proposal to refine the personnel security obligations, including an obligation requiring an AusCheck for critical workers.

The sector has reservations about the capacity of AusCheck to support the proposed expanded CI checking regime; limitations on the use of AusCheck under workplace law; and questions the value of obliging regulated entities to develop and maintain a stand-alone personal security plans.

The sector does not support the use of AusCheck as a pre-employment check for critical workers but would support its use in probation arrangements subject to the Government addressing the identified legislative and resourcing limitations.

Does your organisation have a personnel security plan, or equivalent in place?

Most water sector utilities have implemented background checking arrangements for staff and contractors, primarily through police criminal history checks either coordinated internally or provided by external service providers. Several SOCI regulated entities have adopted the AusCheck arrangements for either critical workers (typically 20-25% of a water utility's workforce) or whole-of-business AusCheck arrangements if the number of workers is small. However, these checks are typically implemented pre-hire or during onboarding, rather than as part of a continuous coordinated personnel security process. A level of ongoing monitoring is provided through fraud and corruption control arrangements combined with ongoing performance management arrangements, but these are not primarily focused on mitigation of the foreign influence and control risks posed by trusted insiders.

Would a personnel security plan requirement improve security posture or duplicate existing controls?

As noted above, most water sector utilities already operate a range of established personnel related controls as part of their broader governance and risk management frameworks. These typically include employment screening, fraud and corruption prevention measures, codes of conduct, disciplinary processes, and access controls for critical assets and facilities. In addition, water utilities apply robust operational controls focused on worker safety, process integrity, and quality assurance, which are essential to maintaining the safety and integrity of drinking water supplies and wastewater services. While these existing arrangements may not be framed explicitly as a standalone 'personnel security plan', they collectively provide a layered, all hazards approach to managing personnel related risks. In practice, these controls mitigate many of the same risks that a personnel security plan would seek to address, including: unauthorised access; inappropriate behaviour; and threats to operational integrity, while remaining closely integrated with operational, safety, and public health obligations.

The sector is concerned that mandating a separate, standalone personnel security plan is unlikely to deliver a demonstrable uplift in security posture relative to existing arrangements. Instead, it risks duplicating controls, increasing administrative burden, and fragmenting established risk management frameworks. This could divert limited organisational capacity

away from core priorities; ensuring continuity of supply and protecting public health through safe, reliable, and secure water and wastewater operations.

Accordingly, the water sector considers that any additional personnel security requirements should focus on recognising, strengthening, or better integrating existing controls, rather than imposing a new parallel framework. A prescriptive personnel security plan requirement, if not carefully aligned with existing operational and safety driven controls, risks shifting emphasis toward managing a theoretical insider threat that the sector has effectively and proportionately managed over many years, without clear evidence of corresponding risk reduction benefits.

Does your organisation currently use background checking as a security control?

As noted above, the majority of water utilities currently use background checking as a security control for both employees and contractors, as part of broader employment screening, safety, and governance arrangements.

While the sector acknowledges that mandating the use of AusCheck for critical water sector workers would introduce greater consistency across critical infrastructure, a number of practical and operational concerns have been identified:

- Lack of portability: The current critical infrastructure AusCheck does not issue a physical or digital CI identity card (unlike aviation and maritime schemes). This limits portability and can result in inefficiencies where workers and contractors are required to undergo multiple AusChecks as they move between projects or utilities. We noted the Department has previously advised that legislative change is required to provide portability but no amendments have been proposed by the Government as part of the SOCI reform package.
- Sponsorship limitations: Critical infrastructure AusChecks cannot be sponsored by non-critical infrastructure entities. This does not align well with the contemporary water sector operating model, which relies heavily on contractors for operations, construction, capital delivery, ICT services, and asset commissioning.
- Timeliness of checks: Delays in receiving AusCheck outcomes can make the process impractical as a pre-employment control. The water sector considers that AusChecks are more workable if it forms part of the business' probation arrangements.
- Employment law implications: A qualified or adverse AusCheck outcome does not provide a defence against unfair dismissal or adverse action legislation. While this is a lesser concern for new hires, it presents material risk when applied to existing staff and transfers legal and industrial risk to utilities.
- Capacity and resourcing concerns: The expansion of critical infrastructure AusCheck requirements, combined with AusCheck's growing role in health, defence industry, global entry, and firearms checking, raises concerns about whether the system is sufficiently resourced to deliver timely assessments. This risk may be partially mitigated by using AusChecks during probation rather than pre-hire. In addition, the sector recommends that the Department establish a preauthorised delivery partner panel to assist with background-checking workloads and improve productivity for industry and the water sector's delivery partners
- Identity verification challenges: The requirement for physical inspection of identification documents is difficult for utilities with geographically dispersed workforces and remote operations. This could be addressed through greater use of digital identity solutions (such as myID/GovID) or distributed verification providers (e.g. Australia Post).
- Foreign worker complexity: Obtaining AusChecks for foreign- or foreign-born workers can be complex and time-consuming, which may constrain access to specialist skills and exacerbate workforce shortages in certain roles--consuming, which may constrain access to specialist skills and exacerbate workforce shortages in certain roles.

In summary, while background checking is already embedded as a security control across the water sector, the sector considers that any expansion of mandatory AusCheck arrangements should be accompanied by reforms that improve portability, timeliness, sponsorship flexibility, and identity verification processes, to ensure the control is both effective and operationally workable. Any rule mandating an AusCheck for critical water-sector workers must be appropriately resourced to minimise AusCheck processing timeframes.

How many AusCheck background checks do you anticipate undertaking each year?

Based on current water sector workforce profiles and feedback from WSSG members that have adopted AusCheck arrangements, it is anticipated that approximately 20–25% of a water utility's workforce would meet the definition of a critical worker and therefore be subject to AusCheck background checks. This proportion reflects roles with unescorted access to critical assets, systems, or operational decision-making functions.-

Applying this assumption to typical workforce sizes reported across the Australian water sector results in the following indicative annual volumes.

- For a small utility servicing 50,000–100,000 connections, with an indicative workforce of approximately 150–300 staff, this equates to around 30–75 AusCheck checks.
- For a medium sized utility servicing 100,000–200,000 connections, with an indicative workforce of approximately 300–600 staff, this equates to around 60–150 checks.
- For a large utility servicing more than 200,000 connections, workforce sizes typically range from approximately 800 to 2,000 or more staff, resulting in an estimated 160–500 or more AusChecks.
- Actual volumes for larger entities may vary materially depending on organisational structure, contractor utilisation, asset dispersion, and the scale of capital and operational programs-

These estimates represent steady state annual activity. Accounting for workforce turnover, new starters, role changes, and contractor onboarding, which suggest that 1,200-3,200 water-sector AusChecks would be required each year, although volumes are likely to fluctuate year to year and may be higher during periods of major capital works or operational change. Accordingly, these figures should be treated as only indicative.

What practical limitations do you foresee for your organisation if required to implement a personnel security plan?

Best answered by individual entities.

Regulatory Impact Analysis

Expenditure data collected by WSAA indicates that each additional $1 million in a water utility's total expenditure requires an additional 1.1 full time equivalent (FTE) water utility employees.

The sector is currently facing a capital investment step change to support housing, asset renewals, response to climate change and regulatory expectations. Forecast capital expenditure for the water sector in 2026/27 is over $11.5 billion, (compared to under $6.5 billion in 2022/23). With the additional expenditure necessary to comply with the proposed cyber, supply chain and physical security measures there will be a commensurate increase in FTE and subsequent increases in AusChecks.

Addendum to the proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules (CIRMP Rules)

Noting the Department's late release of the physical security addendum; the water sector's response addresses the addendum's policy proposals and questions, instead of the questions in the original consultation paper.

In providing this response the water sector makes the following observations regarding the addendum:

- The addendum's terminology is imprecise and demonstrably inconsistent with the SOCI Act. The addendum uses the term 'critical asset' (which applies to the regulated entity concept under the Act) and 'critical systems' (which has no meaning under the SOCI Act). These terms have apparently been applied to what is defined in the SOCI Act as a 'critical component.'. The use of inconsistent terminology creates confusion and risks regulatory overlap.
- Within the SOCI Act construct, it is inappropriate to attempt to mix security controls with safety, public health and operational controls. While the water sector understands and supports an all-hazard approach, it is the responsibility for the regulated entity and should not be mandated through regulatory mechanisms. Any attempt to do so risks duplication and conflict with other existing regulatory frameworks'
- The obligation for continuous monitoring of critical systems (again noting the SOCI Act does not define 'critical systems'), is highly prescriptive and may be cost prohibitive and inappropriate for entities operating geographically disbursed critical components.
- Water sector plants, distribution and reticulation networks (which are presumably what the addendum refers to a 'critical asset') operate within geographically dispersed but integrated networks. These plants and components have long-operational life cycles (typically 50+ years) and were designed in response to the security threat landscape and legislative requirements of that time. Consequently, uplifting physical security controls to reflect the contemporary security environment would require a significant financial investment.

Advice from medium-sized utilities (100,000-200,000 connections) that have undertaken similar security uplift programs suggest that capital expenditure costs of $15-25 million to secure their critical components are typical. Such uplifts include:

- re-construction of sub-standard fences;
- installation of higher-standard fencing at selected sites;
- installation of active security controls CCTV, alarms; access control systems); and
- networking of active security controls.

Additional operational costs are also incurred to monitor and respond to the enhanced security arrangements, typically $500,000-$1.5 million pa depending on the pre-uplifted arrangements. These costs are indicative only and will increase significantly depending on the number of sites, the geographic distribution of the sites, access to telecommunications networks, and infrastructure.

Does your organisation have a physical security plan, or equivalent controls in place?

All water sector utilities have implemented physical security controls to protect their components and operations. These controls are implemented into the multi-barrier controls that ensure the safety and integrity of water and wastewater operations.

Would a physical security plan requirement improve security posture or duplicate existing controls?

The proposed requirements would largely duplicate the water sector's current security arrangements, which are already designed to ensure continuity of supply, protect public health, protect the environment, and ensure service standards. For example, water quality risk-based regulation includes using physical security measures to prevent human contact with water supplies (before and after treatment).

The water sector already considers a range of threat actors and designs appropriate security measures to mitigate physical security risks.

What practical limitations do you foresee for your organisation if required to implement a physical security plan?

Development of security controls is subject to State and Territory legislation. In some jurisdictions, security advice, design and audit of security controls can only be provided by licenced security professionals. Given the limited number of such professionals, it may be impossible for water utilities to comply within the proposed timeframes.

In addition, the water utility three to five-year regulatory pricing cycle, combined with the lead-times necessary to design, construct, commission and operate new physical infrastructure suggest that the proposed 18-month transition timeframe may be impractical. We recommend a 5-year transition timeframe.

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.

Adam Lovell

Executive Director

Water Services Association of Australia

Level 6, 75 Elizabeth Street

Sydney NSW 2000

[redacted]

[redacted]

Luke Sawtell

Industry Co-Chair

Water and Sewerage Sector Group

[redacted]

[redacted]