WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER INDUSTRY SUBMISSION

Protecting Critical Infrastructure and Systems of National Significance – Consultation Paper, August 2020

16 September 2020

Attention: Andrew Kiley
Assistant Secretary
Assurance, Risk and Engagement Branch
Critical Infrastructure Security Division
Department of Home Affairs

SUBMISSION: Protecting Critical Infrastructure and Systems of National Significance, Consultation Paper, August 2020

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

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

We confirm that this submission can be published in the public domain, with the exception of the costings information provided for Question 13 (which is provided as Attachment 1 to this submission).

Background

About WSAA

The Water Services Association of Australia (WSAA) is the peak body that supports the Australian urban water industry. Our members provide water and sewerage services to over 24 million customers in Australia and New Zealand and many of Australia's largest industrial and commercial enterprises. WSAA facilitates collaboration, knowledge sharing, networking and cooperation within the urban water industry. The collegiate approach of its members has led to industry wide advances to national water issues.

About NSW Water Directorate

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

About Queensland Water Directorate

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

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

About VicWater

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

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

About Water Sector Services Group

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

The WSSG has been the coordination point for the water sectors response to the SOCI legislation since its inception and will continue to play a lead role in developing the standard and guidelines that will guide the water sector in its approach to operationalising the SOCI legislative requirements.

Submission key recommendations

The water sector supports the introduction of an enhanced regulatory framework for the Security of Critical Infrastructure Act (2018) and the Government's policy objective of delivering an uplift of security and resilience standards across a range of critical infrastructure sectors. We support key aspects of the proposed approach, particularly the development of the positive security obligations in partnership with the sector, along with aspects of the enhanced cyber security capabilities. We recognise and support the move to improve the protection of our digital networks and a national approach to coordinating communication in relation to cyber security.

Initiative 1: A positive security obligation for critical infrastructure entities

Larger water businesses are State or Territory owned entities with current all hazards obligations. Larger Local Government owned water businesses have similar all hazards obligations. It is important the Positive Security Obligation (PSO) avoids duplication of these existing obligations, including audit and reporting. The PSO must also acknowledge and work with key State, Territory and Local Government based entities including State, Territory and Local Government owners and State and Territory regulators. It is vital that the Department of Home Affairs undertakes genuine consultation with all key stakeholders – water businesses, their owners and State and Territory regulators in the development of the PSO's. The additional support for the Trusted Information Sharing Network (TISN) in this respect is seen as an essential element supporting cross sector development of robust national guidelines and obligations.

It is the sector's position that the regulator would be a State or Territory government nominated entity in the first instance, with the Federal Government providing a last resort option should the State or Territory be unwilling to nominate a State or Territory based regulator.

The documentation provided to date has not differentiated water business licence holders and third party operators of critical infrastructure. Water business licence holders and operations of critical infrastructure can often be the responsibility of separate entities. To remove doubt, any future regulations should address the responsibilities of these entities separately.

Initiative 2: Enhanced cyber security obligations for the entities most important to the nation

The sector has provided a clear definition for entities controlling systems of national significance:

> Critical Infrastructure Entities that if compromised or disrupted would cause significant disruptive impacts on other *Systems of National Significance* in other sectors.

We believe that this definition is of universal application across all critical infrastructure sectors.

The sector assesses that as there are no water sector cross border interdependencies, nor interconnected networks, and the sector operations are inherently resilient, that no water sector entities will constitute *"systems of national significance".*

The need for greater awareness and collaboration on cyber security is agreed. However, there is also a need to contextualise the risk for the water sector, provide clarity on real time data and information requirements, and guidance on the appropriate and proportionate response. Costs to the entity and the customer could be significant depending on the detail of the requirements. The sector welcomes the opportunity to work together with the Department of Home Affairs to ensure measures are proportionate and therefore costs are consistent with good business practice. This may require new capabilities within water sector entities and need to consider State or Territory based regulatory reporting requirements for certain scenarios.

Initiative 3: Government assistance in response to significant cyber-attacks on Australian systems.

The industry understands the need for introducing ‘Step In’ powers into the legislation and that these are a last resort provision only being required when there is a ‘significant, uncontrollable’ cyber-attack on Australian Critical infrastructure. In considering the legislation around these powers we request there are appropriate checks and balances with State, Territory and Local Government owners and regulators to ensure any response is proportionate to the circumstances, aligns with State, Territory jurisdictional response processes, in addition to existing obligations in relation to public safety, customer service and economic benefits. Defining whether a situation is controllable

The sector would welcome the opportunity to work with Home Affairs to determine how to increase the capacity of the sector and provide situational awareness to Home Affairs to ensure that step in powers should not be needed, or if they are that there is a strong collaborative and informed industry base on which to draw for support.

Response to the consultation paper - general aspects

This paper has been produced in response to the consultation paper released by Home Affairs. The parties to this paper welcome the Federal Government's initiative in developing a national approach to protecting critical infrastructure and systems of national significance. We support key aspects of the proposed approach, particularly the development of the positive security obligations in partnership with the sector, along with aspects of the enhanced cyber security capabilities. We recognise and support the move to improve the protection of our digital networks and a national approach to coordinating communication in relation to cyber security.

Policy intent

The water sector is broadly supportive of the Government's policy objective of delivering an uplift of security and resilience standards across a range of critical infrastructure sectors.

However, Government needs to commit to a strong partnership with the water sector to ensure a shared understanding of the threat environment and a contextualised and proportionate approach to the management of these risks within the sector. This includes taking guidance from and supporting industry to improve its resilience through a strong focus on sector interdependencies and an appreciation of sector risk management priorities. This is the best way Government can support improving critical infrastructure resilience for all sectors.

Along with this partnership, the broadening of the application of SOCI to more critical infrastructure sectors would also improve cross sector interdependency risks. However, notably absent is a focus on the Chemical supply sector and Liquid Fuels, which continue to create high external risks to the resilience of the water sector supply chain. In particular, we highlight the essential nature of chlorine for maintaining safe drinking water. The water sector notes that the Commonwealth, through CIPMA, has independently confirmed the critical national supply chain security risk from the single point of failure for liquefied chlorine gas. Any improvement for supply chain resilience in the water sector needs to prioritise resolving these issues.

Regulatory arrangements

Larger water businesses are State or Territory owned entities, responsible to their State or Territory governments and subject to different State or Territory based regulatory regimes. A large number of smaller water businesses are Local Government owned. It is important that Home Affairs recognises this arrangement and does not seek to duplicate existing regulatory and support functions that exist in each State or Territory.

It is important that State or Territory Governments are engaged in the consultation period and a level of consistency for how the water sector is regulated either in each State/Territory or federally is applied. It is important that water sector entities are also able to provide valued input into these arrangements as part of the design of the SOCI standards / regulations for the water sector.

A principles based approach must be developed and clearly articulated to support this. The following are minimum requirements:

a. That where a State or Territory has in place or seeks to introduce to have in place its own arrangements for regulation of critical water infrastructure that these regulatory arrangements will be recognised by Home Affairs. Each State and Territory needs to have the ability to nominate their respective security regulator. In the absence of any nomination then Home Affairs should act as the regulator of last resort, with the agreement of the water business and the relevant jurisdiction.

b. Where there is a conflict between SOCI Act requirements and other State/Territory or Federal Laws then these other State/Territory and Federal Laws will take precedence. For example, we have concerns regarding the management of supply chain risks, particularly in relation to treatment chemicals and liquid fuels. Poorly designed supply chain controls, for example requiring utilities to increase chemical stockpiles, may create a range of dangerous goods risks and conflict with jurisdictional level requirements, such as environmental, safety and dangerous goods regulations.

c. Reporting must seek to complement not duplicate or increase the reporting burden on critical infrastructure water businesses. For example, the proposed calling out of water sector entities captured under the SOCI Act 2018 as *"national security business"* within the Foreign Investment processes provides a live example of potential regulatory reporting duplication in accounting for contracting with foreign owned entities.

Thresholds

Critical Infrastructure Businesses

The current approach to defining a critical infrastructure water business under the SOCI Act is via an arbitrary limit of 100,000 connections. Any proposal to redefine this threshold needs to consider the application of risk based criteria for the sector instead of a lower arbitrary figure. The number of connections threshold has no true bearing to risk and a simple framework (considering the all hazards approach) that accounts for such variables as asset types, distribution networks and high risk uses, could alternatively be adopted in determining the three categories.

Once agreed, the risk criteria would be used to assess the water sector in partnership with industry to define which entities sit in each of the 3 proposed tiers. This should include those organisations covered under Section 51 of the SOCI Act that currently are unable to be disclosed. These lists should then be shared to enable transparent and effective collaboration for all water sector entities on the development and implementation of sector specific standards and guidelines to operationalise these requirements. This will enable a more effective understanding of the context of the entity's classification and requirements under SOCI, which remains blurred within the sector.

If it is not possible to identify entities covered under Section 51 of the SOCI Act, it is essential that these organisations are invited to attend TISN by the Department of Home Affairs to ensure that they have a clear mechanism to learn from others, to enhance their awareness and maturity in managing security risks.

Discussions with Home Affairs indicate consideration of lowering this threshold to introduce greater transparency on reporting entities and capture a number of additional entities. Such a move would increase the number of reporting entities by around 14 or approximately double the current number of reporting entities. Many of these new entities are likely to be low risk, with some having relatively low levels of maturity and capability in risk and resilience management. Providing limited benefit from the additional regulatory effort and the investment cost for these utilities to reach the desired level of maturity.

The definition of the other two tiers of regulatory impact including Systems of National Significance and Critical Infrastructure Entities remains unclear. Based on the definition explained by Home Affairs, it is unlikely there will be any Systems of National Significance within the water sector and the application of Critical Infrastructure Entities seems too broad from an effort / benefit perspective.

As part of this consultation with Home Affairs, WSSG and WSAA developed and provided a proposed set of options for setting SOCI thresholds for the water sector. Option 1 outlines the sectors preferred approach to utilise risk based criteria to assess the sector and then confirm and share the lists of water business within each tier of the legislative requirement. We believe a similar approach could be adapted across all sectors.

Systems of National Significance

The threshold for selecting Systems of National Significance is currently unclear. The primary criteria relate to impacts at a national level and interconnectivity. Systems of National Significance for the water sector (and possibly all sectors) should be defined as:

> Critical Infrastructure Entities that if compromised or disrupted would cause significant disruptive impacts on other *Systems of National Significance* in other sectors.

The sector assesses that as there are no water sector cross border interdependencies, nor interconnected networks, and the sector operations are inherently resilient, that no water sector entities will constitute *“systems of national significance”*

All hazards approach

The adoption of an all-hazards approach to risk is commended. However, most water businesses covered by the SOCI Act currently are subject to a range of existing all-hazard regulatory service delivery requirements through: emergency management; dam safety, public safety and security requirements; drinking water and waste water quality standards; land management and bushfire risk reduction requirements; work health and safety requirements; privacy; chemical storage and security; and customer service obligations. While not explicitly focused on security, these obligations do provide a genuine all-hazards approach to management of risk, with security controls regularly included as a risk mitigation. The new SOCI Act obligations must not seek to replicate, or conflict, with these arrangements.

Water utilities typically operate over a broad geographic area. Whilst some aspects of the entity such as cyber security and supply are likely to be centralised, hazards relating to people and physical aspects may differ depending on the nature of the facility and its location. The SOCI arrangements must explicitly acknowledge that decisions regarding the appropriate balance of risks and the application of proportionate controls and mitigations are a matter that the utility licence holders, their existing regulators and owners are best placed to manage, and have always managed as *"business as usual"* to support their normal service delivery obligations.. Setting principles based outcomes within the legislation then enables sectors to determine and document best practice approaches to how these outcomes would be best achieved in the water sector. These would then be documented within the standards and guidelines to inform the supporting regulations for the water sector.

The Federal Government has proposed that the compliance with the all hazards approach will be through an annual board level endorsement to assure that the utility is compliant with the requirements of the SOCI Act. To ensure that risk mitigation efforts are appropriately prioritised and targeted, the industry welcomes the proposed discussions through TISN on appropriate risk context statements; best practice guidance and/or recommended standards.

Positive security obligations (PSO)

The sector welcomes the application of Principles Based controls being proposed as part of the PSO that would apply to Regulated Critical Infrastructure Entities. This ensures that instead of prescriptive regulated controls being set, the water sector can define sector specific, contextualised and proportionate risk controls that meets the principles set out in the legislation. The engagement with industry to codesign the standards and guidelines that will outline the approach to operationalising these requirements within the sector is also supported. This will enable experts within each sector to work collectively with Government through the TISN groups like the WSSG to develop the supporting SOCI regulation for the sector.

The proposed approach retains strong compliance and enforcement elements that potentially undermine cooperative and collaborative engagement. We request Government commit to the implementation of a no-blame, just culture approach as a principle underpinning the regulatory design.

Given the State, Territory and Local Government ownership of water businesses it is envisaged that the PSO's would apply in a manner similar to national Health and Safety legislation, where the Commonwealth establishes good practice, in consultation with the sector that is then adopted by each State and Territory jurisdiction.

In terms of the supply chain we highlight that the water sector is quite reliant on chemical manufacturing and liquid fuels. At present there is no formal recognition of chemical manufacturing or liquid fuels under SOCI. The water sector notes that the chemical and fuels sector were included in international critical infrastructure frameworks since their inception and believes that this is a significant omission that must be addressed through the current consultation review.

Enhanced cyber obligations

The industry broadly supports the move to enhance the cyber security maturity of Australia. We welcome the concept of working with the industry to increase preparedness and response capabilities provided these are done in conjunction with State, Territory and Local Government jurisdictions to avoid duplication and effectively leverage existing initiatives, with a view to propagating good practice across the industry at a national level.

The cyber threat to the water sector needs to be appropriately contextualised by Government. Unlike electricity and communications networks, the physical design of water and wastewater systems provides a level of resilience to disruption. Consequently, the sector's cyber obligations must be commensurate with the level of sectoral risk and the potential consequences which are demonstrably lower than other utilities.

A better understanding of the scenarios and requirements for cyber security reporting obligations and request for the provision of real time data / information relating to cyber security incidents is required. This may require new capabilities within water sector entities and may also need to consider State and Territory based regulatory reporting requirements for certain scenarios.

The industry understands the need for introducing 'Step In' powers into the legislation and that these are a last resort provision only being required when there is a 'significant, uncontrollable' cyber-attack on Australian critical infrastructure. In considering the legislation around these powers we request that there are appropriate checks and balances with government owners and regulators to ensure that any response, is proportionate to the circumstances, public safety, customer service obligations and economic benefits.

We acknowledge that the question of whether a situation is controllable or uncontrollable may be uncertain (particularly in the immediate aftermath of an attack) or could become a source of disagreement between government and the sector/entity. However, we would assume that this can be minimised through a history of engagement between government and the entity that has built trust and a culture of mutual understanding. Clearly, engagement, mutual respect and empathy are important considerations here.

There has been a suggestion from the Department of Home Affairs that entities that are contracted by or form part of the supply chain for water businesses would be captured by the Step In powers. This may cause sovereign risk to these entities who may be completely unaware they are covered. The cyber risk from these entities falls into two categories: 1) entities directly contracted to run assets owned by the water business and 2) entities involved in supply of goods or services to water businesses. The water sector believes that the Step In powers should only apply to licenced water businesses, not their subcontractors or supply chain.

Including subcontractors or the supply chain creates risk and uncertainty which can be more appropriately managed through the PSO's and direct engagement via the water business who has the direct contractual relationship. It is the water business who is accountable to the regulator, government and the customers and therefore owns the risk. The need for real time reporting is acknowledged. However, it needs some definition on the exact timeframe e.g. as things evolve, within 24 hours or longer. Further clarification is required to define the threshold of cyber incidents that need to be reported, how they are reported, to who they are reported, and when the Government would step in. This may require new capabilities within water sector entities and will need to consider State and Territory based regulatory reporting requirements for certain scenarios. Noting the real risk of duplication where State, Territory or Local Government owned water entities are reporting to their jurisdictional Governments on cyber risk and incident matters.

The sector would welcome the opportunity to work with Home Affairs to determine how to increase the capacity of the sector and provide situational awareness to Home Affairs to ensure that Step In powers should not be needed, or if they are that there is a strong collaborative and informed industry base on which to draw for support.

Prior to these reforms, the Government had not recommended or mandated any specific information technology or operational technology security standards for the water sector. As a result, utilities have adopted international standards and international practices based on their assessment of the risk. While we support the provision of best practice advice by Government, the Principles Based outcomes for Information and Cyber Security outlined as part of the PSO are adequate to enable a level of assurance being provided to Government. Compliance with specific standards should not be mandatory as organisations have approached these requirements through various standards and best practice guidance.

The Government has not recognised that water sector representatives have been long standing active committee members of international operational technology security forums (DNP3 OT International Security Committee) and utilises these higher level standards. Prescriptive direction in this space may create further financial impacts and regulatory burden for water sector entities. In addition, prescriptive standards are typically inflexible and difficult to keep up-to-date. This is of particular concern in the cyber-security space where prescriptive standards could be out of date by the time they are published. Potentially increasing business risk. Best practice guidance for the water sector would be defined in the industry co-designed standards / regulation which are outcome focus. Noting that any mandatory standard above the currently assessed response level is likely to result in significant business cost and lengthy transitional processes.

Government assistance needs to be better contextualised through scenario based examples for the water sector. This is important to understand the likelihood, conditions and approach that Government would take if they deemed a water sector organisation needed direct Government intervention to manage a cyber event. The water sector would welcome the opportunity to work with Home Affairs to develop this awareness.

Role of the Trusted Information Sharing Network (TISN)

The TISN and its supporting sector groups bring together the security and resilience subject matter experts from across each sector, with a shared focus on improving resilience within the sector and in turn their organisations. The water sector supports enhancing the role of the TISN, particularly the stronger focus on education and engagement activities, utilising it to co-design industry best practice guidance, including event specific response plans and industry vulnerability assessments and strengthening the engagement and awareness of the TISN with Boards and Executives. The role of the TISN is vital to define industry context for Government and to translate Government policies like SOCI into valued, proportionate and effective industry outcomes.

The water sector notes with concern that the leadership and management of the TISN by the Government regulator (DHA-SOCI) creates a measurable *"conflict of interest"* and directly compromises the *"trusted information sharing"* environment. This significant conflict of interest must be addressed as a priority, for the water sector to continue with active participation under the current TISN model. This would occur through joint discussion with the Department of Home Affairs, WSSG and WSAA. Full participation can only continue where there is a genuine spirit of collaboration within no blame, just culture principles.

However, the sector notes that the Government's resourcing and support for the TISN has progressively reduced over time, while expectations for policy engagement, exercise participation, regulatory co-design and cross-sector engagement have increased, together with the introduction of the regulatory “conflict of interest” dimension. The water sector’s capacity to fund increased TISN activities is limited by the sector’s price controls, and suggest the Federal Government assume responsibility for funding TISN activities, particularly those activities that primarily benefit the Government, such as co-design and cross-sector initiatives.

The water sector also notes that there was neither consultation nor review with the sector of the recent sector threat analysis and risk context statements (water sector risk context statement and the cyber risk statement for the water sector), before publication, leading to inaccuracies. In the past the water sector was always engaged by agencies in the production and review of sector specific threat and risk context statements. The outline of further investment into the redesign and operation of the TISN by Government is welcomed, as these groups need to be better supported as the primary engagement point with industry on the matters covered under SOCI and the national Critical Infrastructure Resilience Strategy. In redesigning the TISN, it is critical that the “DHA regulatory conflict of interest” issue is resolved, to enable the role of sector groups to be maintained and enhanced to support a broadening of security and resilience principles such as those in SOCI and an elevation of maturity across all entities within the sector, especially those that will be subject to SOCI. If supported and enhanced, the sector groups can deliver on the outcomes Government is seeking from SOCI and more importantly sector specific approaches and outcomes for improved security and resilience.

In support of the sector groups, the TISN also needs to structure a work program of activities and forums that continually improve understanding and capability of cross sector interdependencies. These could be threat vector based where the right people from each relevant sector come together to learn and work on shared improvements and capability uplifts. This will also support direct interaction with TISN groups outside of Home Affairs, with the varied government departments that seek to engage the water sector for specific activities and intelligence sharing.

In forming these groups care must be taken not to duplicate existing structures within the water industry through the national peak body the Water Services Association of Australia, and State based sister organisations (the Queensland Water Directorate, NSW Water Directorate and VicWater). WSAA in particular has had an ongoing interaction with the TISN through the Water Services Sector Group (WSSG). It also has in place a number of existing vector/subject matter based expert groups representing all major water utilities and the majority of water businesses with greater than 25,000 property connections who come together for the purpose of sharing, learning and developing robust national guidance. It is both sensible and to avoid duplication to ensure WSAA maintains a strong partnership with the WSSG and the TISN and to provide a more efficient mode of engagement and deliver, whilst ensuring that the water sector leadership retains direct oversight of progress.

Improving engagement with State, Territory Government and Local Government representatives must be considered as a high priority for TISN enhancements, to ensure a shared focus and understanding between industry and all layers of Government. A model for the TISN structure going forward that has been previously proposed by WSSG would create a much stronger focus on the State and Territory Jurisdictional arrangements that would in turn improve national outcomes, and avoid duplication with current State and Territory based mechanisms, as follows:

- Each State and Territory develops their own State or Territory based TISN and Critical Infrastructure Resilience Strategy within their own context and arrangements.
- State or Territory based sector groups are established where there is more than one entity in that sector providing services within the State or Territory. Each State or Territory nominates a single representative to attend State or Territory based cross sector group meetings and the national TISN sector group. Where there is a State or Territory based Sector group this representative would most likely be the Chair. Where there is a single sector provider for a State or Territory then that provider would nominate a national representative.
- State or Territory based cross sector groups are established made up of the State or Territory nominees from each sector group. These groups would also include Emergency Management, Policing and Cyber representatives from the State or Territory government.
- At a national level TISN would comprise of the Sector representatives from each State or Territory. This national group would provide a vehicle for information sharing on security issues, situational awareness for issues which cross State or Territory boarders and potential coordination for resources that cross State or Territory borders, along with addressing mutual aid requests.
- The make-up then of the Critical Infrastructure Advisory Council (CIAC) would include:
    - Federal Government – Home Affairs
    - State or Territory Government representatives – as nominated by each State or Territory
    - National TISN Sector Group Chairs – as nominated by each sector group
- The role of CIAC is enhancing critical infrastructure resilience by streamlining and sharing processes, intelligence and approaches between sectors. The role of TISN is to coordinate across sectors at a national level for events that cross State or Territory boundaries or that are of national significance. Guidelines and frameworks developed at a Federal level would be robustly tested across each State or Territory jurisdiction. However, it would be the discretion of the State or Territory as to whether they adopt and Federal guidelines, or frameworks and the extent of any such adoption.
- Peak industry bodies should be engaged as a valued partner at all levels of the Federal and State/Territory TISN/CIAC arrangements as relevant to the sector.
- The current weakness with CIAC is that it doesn't have a direct line of ministerial reporting, we recommend that CIAC reports to the relevant ministers responsible for critical infrastructure under the new National Cabinet structure. This is to separate policy development and resourcing from direct regulatory responsibilities. This would also support enhancing the engagement and outcomes with States, Territories and Local Government.

The benefit to this model is that majority of water business licence holders remain engaged at the State and Territory jurisdictional level where management of incidents and emergencies occurs, enabling more meaningful change and growth can occur. This grows the maturity of the TISN from the ground up.

The role of the Department of Home Affairs as the purveyor of the TISN and as the SOCI regulator also needs to be considered further, as the fundamental "trusted sharing" environment is measurably compromised creating the risk of regulatory penalty, arising from open discussions within the TISN environment.

In a no-blame, just culture principle, membership of, and engagement with, the WSSG would be considered prima facie evidence of an appropriate security culture from within a water business.

Compliance costs

In the absence of details of the proposed regulatory regime, it is difficult to estimate the potential compliance costs for each water business. However, it’s envisaged that additional costs would be incurred in terms of security personnel (in-house or outsourced) along with capital and operational expenditure. Ongoing compliance with the cyber-security element and other elements of the positive security obligations may also result in an increase to annual operating costs. Based on experiences in the airline sector these costs can be significant and increase as the business reaches full compliance maturity. The sector would welcome the opportunity to explore the associated economic modelling for the water sector with the Department of Home Affairs as part of ongoing consultation prior to the development of any regulations or guidelines.

The information provided by Home Affairs through discussion forums indicates the view that the costs are part of good business management. This is true provided that the requested measures are fair and reasonable. If we take cyber security as an example, international standards such as IEC 62443 note several levels of security prevention. Attainment of the highest level of security under this framework requires significant system duplication, which at present would be considered by the industry as disproportionate to the risk, and result in an impost in the order of tens of millions of dollars. Implementation of cyber security measures and attainment of the positive security obligation to a level considered good practice for a medium sized water utility is estimated to add between $1.0 to 1.5M to business costs, which will need to be passed on to customers. This cost is estimated to be orders of magnitude higher for large organisations.

Implementation and timing

The exact timing for implementation of measure to attain the PSO and any Cyber Security obligations will depend on the exact requirements. However, the water industry would expect that there would be a period allowed for effective implementation proportional to the cost and effort. If the requirements are of significant cost or complexity then an implementation period of years will be necessary, as expenditure approvals are prioritised by the sector owners (State, Territory and Local Governments). At the minimum the industry would request a 12 month initial implementation period with the provision of a SOCI gap analysis roadmap for each sector to be presented at the end of that 12 months, with consultation, review and approval by the jurisdictional regulators, Owners (State, Territory and Local Governments) and Boards. As long as the sector and organisations have approved plans agreed with their jurisdictional regulators and Owners (State, Territory and Local Governments), this should be acknowledged, and no penalties applied.

Detailed response to the consultation paper questions

Coverage

Q1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing?)

The water sector is quite reliant on chemical manufacturing and liquid fuels. Addressing security risks from these sectors under current arrangements may require stockpiling of quantities of hazardous materials. Including these sectors under SOCI would provide greater resilience for water businesses, and reduce overall community risk associated with stockpiling of hazardous material. In addition, we believe these sectors to be critical to the functioning of other CI Sectors including Defence, Energy, Space and Transport. While Liquid Fuels is represented within the TISN structure as part of the Oil and Gas Security Forum, the chemical sector is not.

In particular, we highlight the essential nature of chlorine for maintaining safe drinking water. The water sector notes that the Commonwealth, through CIPMA, has independently confirmed the critical national supply chain security risk from the single point of failure for liquefied chlorine gas. We would welcome the review and inclusion of the chemical sector within the TISN structure and further assessment of the application of the SOCI legislation to the sector.

In addition, consideration should be given to inclusion of:

- Chemical manufacturing including liquid fuels
- Mining
- Technology and innovation industries including university research institutions – this should be split from education.

Q2. Do you think current definition of Critical Infrastructure is still fit for purpose?

- Although the current definition continues to have utility, there is considerable value in replacing it with a graduated or hierarchical classification scheme as advanced in Figure One of 'Protecting Critical Infrastructure and Systems of National Significance Consultation Paper' (August 2020) (Consultation Paper).
- This comment is on the assumption that the allocation or classification is based upon the application of objective and measurable criteria in consultation with the applicable entity.
- The current definition of Critical Infrastructure is quite broad. It would benefit from a number of clarifying definitions, particularly for 'extended period' and 'significantly impact'. Clarity should also be provided on the parameters around the 'social or economic wellbeing of the nation'.

Q3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

- The assessed average time it will take for the entity to recover in the event of a major security incident (such as a cyber-attack).
- Whether the impact of a cyber incident actually manifests into an extended community service delivery disruption.
- Whether the entity has inherent or intra-sector redundancy such that its critical outputs can be replicated.
- Situational threat dependencies that span across sectors, e.g. water is reliant on electricity and telecommunications, if a credible threat to the energy and/or telecommunications sectors is identified the water industry should be advised what level of risk that presents to service provision so we can prepare contingency, ramp up resources or stage equipment at critical assets.

Q4. What are the common threats you routinely prepare for and those you have faced/ experienced as a business?

While the terms 'threat', 'hazard' and 'risk' are sometimes used interchangeably in the Consultation Paper, there are some common threats that are 'top of mind' for the entity. Regulators and intelligence providers need to adopt a common or shared vernacular with the possible incorporation of terms such as attack pathways and methods of attack.

In terms of business resilience, the water sector customarily adopts an all hazards approach. That is, natural hazards such as fire, storm, flood, earthquake, landslip, erosion (for example) and terrorism, pandemic, industrial & community action, cyber, loss of dependency such as electricity, telecommunications, chemicals and failure of critical suppliers have generic business continuity plans.

The threats are:

- Social engineering of staff
- Trusted insider
- Technology partner networks and services
- Non-standard equipment hampering contingency support
- Country of manufacture
- Catastrophic asset failure
- Natural events and disasters
- Cyber attacks
- Critical supply chain failures
- Step in rights for poorly managed water & wastewater systems
- Acute regulator changes that can impact business decisions and costs
- Geopolitical changes

Q5. How should criticality be assessed to ensure the most important entities are covered by the framework?

For the water sector we propose the application of risk based criteria to define the Critical Infrastructure Entities that sit within each Tier of the SOCI framework as follows:

Systems of National Significance – Water Sector (only if applicable to the water sector)

- Critical Infrastructure Entities that if compromised or disrupted would cause significant disruptive impacts on other *Systems of National Significance* in other sectors.

CI Regulated Entities – Water Sector

- Entities which if compromised or disrupted would have a significant impact on the city / region they service and/ or other Regulated CI Entities from other sectors.
- This should then also include the Entities currently covered under Section 51 of the SOCI Act.

Other CI Entities – Water Sector

- A water entity that holds an operating licence for the commercial provision of water services with their State, Territory or Local government (this would capture raw water, stormwater etc. including entities under the NSW WICA Act).

With significant being defined as such a level that a State or Territory government has declared a State of Emergency or State of Disaster due to the impact on or caused by the water service provider.

The water sector would work with Home Affairs to develop a risk based criteria to support the assessment of the organisation as the asset and which of the 3 tiers it falls into. Water organisations would then utilise a model to assess the elements of their organisation/assets to define criticality.

Q6. Which entities would you expect to be owners and operators of systems of national significance?

That would depend upon the objective application of agreed criteria, which ideally would be conducted in consultation with the sector and the entity. The proposed criteria put forward by the sector, as noted above is:

> Critical infrastructure entities that if compromised or disrupted would cause significant disruptive impacts on *Systems of National Significance* in other sectors.

Under this definition it is considered unlikely that any water business will meet the threshold for *Systems of National Significance*.

Uplift in government support for critical infrastructure

Q7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

A refreshed and effective TISN should be the number one priority for government to ensure effective industry engagement to operationalise the requirements of SOCI. If the TISN was working effectively as a trusted partnership like it did in its initial years, it is unlikely that the SOCI legislation would have needed to be created.

Home Affairs should prioritise revitalisation of all sector groups as a valued partner for government and enable them to define and deliver on the outcomes the government is seeking in a context and proportionate approach that works for their industry. A critical component of this in a renewed and consistent engagement and relationship with States, Territories and jurisdictions as a critical component of this partnership.

The development of a refreshed Critical Infrastructure Resilience Strategy needs to be easily translatable into sector specific work programs along with State, Territory and Jurisdictional outcomes. It also needs to integrate with existing State or Territory based strategies such as the NSW Critical Infrastructure Resilience Strategy. This needs to provide a top down / bottom up approach.

Key considerations for the TISN, CIR Strategy and WSSG:

TISN

- Continuation and establishment of TISN sector groups for all sectors covered under SOCI along with others that already exist.
- Proportionate engagement with the TISN for entities that are subject to SOCI should be outlined as a requirement and further defined for each Tier in each sector within the co-designed regulations.
- Recognition and resolution of the actual Regulatory “conflict of interest” with DHA as the owners of the TISN.
- Strong support and resourcing to get all sector groups functioning well and delivering on outcomes for their sector.
- Strong focus and resourcing from Home Affairs on cross sector interdependencies and operationalising outcomes of inputs from sectors.
- Increase in Home Affairs TISN resourcing model by supporting sector groups to do the heavy lifting with dedicated staff to maintain the administrative and coordination side of a continued sector group agenda.
- Improved provision of threat intelligence/information that is tailored to sectors and (ideally) entities, which is relevant, actionable and timely.
- Work collaboratively with the sector and entities to define collection plans based on a shared understanding of the sector and its needs.
- Receive and act on feedback concerning the utility of information.
- Increased collaboration and sharing.
- The WSSG would be a key enabler to uplift maturity in the sector and utilise the combined knowledge, experience and skills to produce guidance materials and standards.

CIR Strategy

- Clearly defined strategy that is easily translatable into key focus areas that sectors, States, Territories and jurisdictions can adopt and deliver on actionable outcomes.
- Principles based outcomes focussed to ensure the strategy is not prescriptive but can be measured within sectors and jurisdictions.
- Supported by an annual program of work that is driven by Home Affairs and is correlated to sector specific work programs and jurisdictional initiatives.
- Complements other existing strategies e.g. Cyber Strategy.

Critical Infrastructure Advisory Council of Australia (CIAC)

- Reshape CIAC to ensure consistent memberships across all sectors and jurisdictions. States, Territories and jurisdictions have 3 key functions that need to be represented in the CIAC discussion including:
    - Critical Infrastructure Policy (e.g. First Ministers Departments)
    - Security (e.g. Police)
    - Emergency Management (e.g. Emergency Services)
- Jurisdictional representatives either need to represent all these functions or someone from each of those functions from each jurisdiction should be engaged to support the improvement of these networks in a critical infrastructure context. This will support strengthening understanding of critical infrastructure disruption risk and response.
- A fourth representative for the relevant cyber function from each State and Territory jurisdiction could also be considered.
- CIAC must be focused on an awareness of CIR efforts in each sector / jurisdiction but most importantly on the delivery of the CIR Strategy and underpinning work plans that are focussed on interdependences.

WSSG

- Provide or enable the WSSG to find an effective secretariat function and resourcing that can coordinate activities and support a continued agenda.
- Support the WSSG to become a key enabler to uplift maturity in the sector and utilise the combined knowledge, experience and skills to produce guidance materials and standards, through a dedicated work program.
- Consideration of formal relationship with the Water Services Association of Australia to more directly support the WSSG. Particularly in being able to coordinate resources and expertise from across the water sector, along with direct engagement with Managing Directors and Senior Executives from all major water businesses across the country. WSAA has had an ongoing interaction with the TISN through the Water Services Sector Group (WSSG) for many years. It also has in place a number of exiting vector/subject matter based expert groups representing all major water utilities and the majority of water businesses with greater than 25,000 property connections who come together for the purpose of sharing, learning and developing robust national guidance. It is both sensible and to avoid duplication, to ensure WSAA maintains a strong partnership with the WSSG and the TISN and to provide a more efficient mode of engagement and deliver, whilst ensuring that the water sector leadership retains direct oversight of progress. In addition, depending on the operating model for TISN going forward, working with WSAA would provide opportunity to address the current regulatory ‘conflict of interest’, through the sector engaging via the association.

Q8. What might this new TISN model look like, and what entities should be included?

- Sector groups to be expanded to include all sectors covered under SOCI along with an additional existing or required.
- All entities covered by SOCI, including those covered by a Section 51 notification. These entities in particular need to be invited to TISN to enhance their understanding, maturity and ability to deliver.

- Improved sector group engagement facilitated through the inclusion of the need for entities covered under SOCI to be engaged.
- Proportionate TISN / Sector group memberships aligned to the hierarchy of critical infrastructure tiers (see Figure One of the Consultation Paper) so that the degree of support (provision of information and intelligence) is accurately and objectively calibrated to need.
- The level of engagement expectation would be proportionate to the scale of the entity.
- CIAC with consistent membership.
- Resilience Expert Advisory Group engaged and resourced with an annual work program to deliver outcomes for CIAC on cross sector and sector specific deliverables.
- Cross sector focussed forums, projects and activities based on shared focus on priorities from the CIR strategy and shared threat vector themed.
- Ensure that industry specific issues are captured and linked to TISN's broader scope, and to provide end-to-end cross sector coverage (e.g. transport and supply chain management of treatment chemicals).

A model for the TISN structure going forward that has been previously proposed by WSSG would create a much stronger focus on the State, Territory and jurisdictional arrangements that would in turn improve national outcomes, and avoid duplication with current State or Territory based mechanisms, as follows:

- Each State, Territory and jurisdiction develops their own state based TISN and Critical Infrastructure Resilience Strategy within their own context and arrangements.
- State or Territory based sector groups are established where there is more than one entity in that sector providing services within the State or Territory. Each State or Territory nominates a single representative to attend State or Territory based cross sector group meetings and the national TISN sector group. Where there is a State or Territory based Sector group this representative would most likely be the Chair. Where there is a single sector provider for a State or Territory then that provider would nominate a national representative.
- State or Territory based cross sector groups are established made up of the State or Territory nominees from each sector group. These groups would also include Emergency Management, Policing and Cyber representatives from the State or Territory government.
- At a national level TISN would comprise of the Sector representatives from each State or Territory. This national group would provide a vehicle for information sharing on security issues, situational awareness for issues which cross State or Territory boarders and potential coordination for resources that cross State or Territory borders, along with addressing mutual aid requests.
- The make-up of the Critical Infrastructure Advisory Council (CIAC) would include:
    - Federal Government – Home Affairs
    - State or Territory Government representatives – (as nominated by each State or Territory)
    - National TISN Sector Group Chairs – As nominated by each sector group

- The role of CIAC is enhancing critical infrastructure resilience by streamlining and sharing processes, intelligence and approaches between sectors. The role of TISN is to coordinate across sectors at a national level for events that cross State or Territory boundaries or that are of national significance. Guidelines and frameworks developed at a Federal level should be robustly tested across each State or Territory jurisdiction. However, it would be the discretion of the State or Territory jurisdiction as to whether they adopt and Federal guidelines, or frameworks and the extent of any such adoption.
- Peak industry bodies should be engaged as a valued partner at all levels of the Federal and State TISN/CIAC arrangements as relevant to the sector.
- The current weakness with CIAC is that it doesn't have a direct line of ministerial reporting, we recommend that CIAC reports to the relevant ministers responsible for critical infrastructure under the new National Cabinet structure. This is to separate policy development and resourcing from direct regulatory responsibilities.This would also support enhancing the engagement and outcomes with States and Territory jurisdictions.

  The benefit to this model is that majority of water business licence holders operators remain engaged at the State, Territory and jurisdictional level where management of incidents and emergencies occurs and more meaningful change and growth can occur. This grows the maturity of the TISN from the ground up.

Q9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

- Strengthen the TISN to in turn strengthen the security and resilience aspects of each sector.
- The establishment of jurisdictional based arrangements as noted in the response to Question 8, to ensure that risks are contextualised and appropriately addressed for the jurisdiction involved.
- All participants should play to their strengths – government has extensive resources, the ability to assess and articulate geopolitical threats and the remit to exercise control while entities understand their industries, know their vulnerability and working with government can develop a sound understanding of their risks
- Government could provide a cyber security service to smaller entities that do not otherwise have the resources to adequately protect themselves.
- Funding and cost recovery in circumstances where mandated requirements are either above and beyond the ability of an entity to resource or are the result of actions outside of the control of the entity.
- Support each sector to articulate and develop a minimum set of security standards that have been formulated in consultation with the sector and are proportionate and reasonable.
- Consult with the sector State, Territory and Local Government Owners regarding the most appropriate integration of security principles into existing regulatory frameworks.
- Provide information on typical risks and vulnerability within the sector, which otherwise may not be able to be sourced because of competition risk

- Addressing gaps in sector continuity planning/plans, e.g. most sectors are not adequately prepared for water outages.
- In managing cross State or Territory emergencies water utilities need clear powers to at efficiently in the best interest of the community where there are grey areas in relation to jurisdictional control.
- Improving focus on community resilience and facilitating discussion around outage tolerance, i.e. communities in rural areas are more resilient and able to cope with outages compared to their city equivalents.
- More robust discussions need to be had around customer's willingness to pay for improving service/operational resilience and corresponding pricing submissions with regulators - government can facilitate those discussions with pricing regulators for State, Territory and Local Government owned corporations.
- Leverage well-established State, Territory and Local Government based security frameworks.
- Added focus on training programs for organisation-wide security awareness.
- Communication of government risk based prioritisation between sectors.

Positive Security Obligation

Q10. Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

Yes, the principles proposed are quite clear. The water industry supports the focus on physical, cyber, personnel and supply chain security. Along with the approach of ensuring effective governance and oversight to identify and mitigate risks with the outcome of minimising incident impacts. It is very important that any associated regulation would be via the relevant regulator, with an emphasis on outcomes and avoiding compliance burden.

To this end the security obligations must align with current State or Territory regulatory provisions to avoid duplication, contraction or inefficiencies. We recognise the significant benefit of shared intelligence and its role in strengthening national security.

Whilst Department of Home Affairs will have national jurisdiction, the State or Territory regulatory bodies' jurisdiction and role in dealing with incidents must be factored into incident response planning for a more synchronised incident management protocol.

Q. 11 Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

- Yes, they are sufficiently high-level yet explicit enough to provide effective guidance for the drafting of sector specific standards – they also align to existing PSPF.
- Notwithstanding the desirability of having 'room to move' in terms of obligations, there is still a strong desire to agree upon a single set of standards that are achievable, proportionate and reasonable – this provides surety and gives the entity an ability to plan and forecast security costs.
- It is important that the PSO's recognise existing State, Territory and Local Government obligations. For example, Victoria has the Victorian Protective Data Security

Framework (VPDSF), a framework that covers the areas suggested by the Positive Security Obligations, and is already well embedded. Further, they are currently establishing a water sector wide group (under VicWater governance) to ensure appropriate emphasis of this framework is applied to Operational Technology. The implementation of this group is supported by Victorian water business Managing Directors.

Q12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

Water businesses currently covered by the SOCI Act are subject to a range of existing all-hazard regulatory requirements through: emergency management; dam safety and security requirements; drinking water and waste water quality standards; land management and bushfire risk reduction requirements; work health and safety requirements; privacy; and customer service obligations. While not explicitly focused on security, these obligations do provide an all-hazards approach to management of risk, with security controls regularly included as a risk mitigation. The new SOCI Act obligations must not seek to replicate, or conflict, with these arrangements.

However, the current principles are quite broad and the supply chain security obligation in particular is very loosely defined. Any costing to meet the obligation requires more detail on the individual sector requirements. For example: the cyber security obligation is highly dependent on the level of cyber security controls required. The time to implement controls could vary from none to two or three years depending on the exact nature of the controls. Similarly, the cost could vary from minimal to tens of millions of dollars. The only way that this can be determined accurately is after the detail of the requirements have been agreed.

Q.13 What costs would organisations take on to meet these new obligations?

Please refer to Appendix A.

Q14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

Yes. Two examples, one from the aviation sector the other from the water sector.

We understand the Aviation Sector (private and public) also experienced the introduction of positive security obligations from September 2001 onwards. Over a period of 10 years from 2001 to 2011, annual Commonwealth aviation security funding grew from a baseline of $21 million annually in FY 01/02 to almost $300 million in FY 11/12. In the same period, security functions in a major Australian airline doubled in size and security costs rose proportionally in tandem with government aviation security spending as industry and government shared the financial burdens. The continuing cost to industry was significant once all additional physical, people and digital security programs were introduced.

While the imperatives for growth may now be different, the general lessons remain valid and extant. Based on that experience, it is clear that the initial costs of hardening and monitoring of physical assets, vetting and monitoring of personnel, enhancements to the supply chain and upgrades associated with cyber security, along with the cost of audits and compliance, will likely be significant. While ongoing costs will be significant, there is also a history of scope creep and inclining costs until full maturity is reached, noting that this may take 5-10 years.

It should be noted the response in the aviation sector during the 2000's was proportionate to a known, credible and increasing threat to national security. This does not currently exist, nor has it existed in the past for the Australian water sector. Therefore we would reinforce that any costs in relation to meeting an increased security obligation need to be proportional and based on a realistic assessment of the threat level. Another factor to consider is that unlike private sector entities, public water utilities cannot immediately pass on the costs of new measures to their customers due to the nature of the pricing and regulatory environment within which they operate. This means that supplementary funding will likely be required from government for unforecast or immediate measures required outside of the four or five year price determination cycles.

Sydney Water has also to an extent been subject to a security obligation, which is expressed in Clause 9 of its Operation Licence 2019 - 2023 – these provisions align with aspects of the Security of Critical Infrastructure Act (2018), which is also reflected in recent structural changes in the organisation.

Regulators

Q15. Would the proposed regulatory model avoid duplication with existing oversight requirements?

The proposed regulatory model is quite high level. Unfortunately, it fails to detail the interaction with existing regulatory mechanisms and obligations. Larger water businesses are State or Territory owned entities, responsible to their State or Territory governments and subject to different State or Territory based regulatory regimes. Smaller water businesses are a mix of State, Territory and Local Government entities. It is important that Home Affairs recognises and doesn't seek to duplicate existing regulatory and support functions that exist in each State or Territory. A principles based approach must be developed and clearly articulated to support this.

The following would be minimum requirements:

- A single State or Territory based regulator must be nominated to avoid duplication with existing oversight requirements and resolve compliance with existing State or Territory obligations.
- Where a State or Territory has in place or seeks to introduce its own arrangements for regulation of critical water infrastructure that these regulatory arrangements will have primacy and will be recognised by Home Affairs. Each State or Territory needs to nominate their respective security regulator. In the absence of any nomination then Home Affairs should request nomination.
- Where there is a conflict between SOCI Act requirements and other State, Territory or Federal Laws then these other State, Territory and Federal Laws will take precedence. For example, we have concerns regarding the management of supply chain risks, particularly in relation to treatment chemicals and liquid fuels. Poorly designed supply chain controls, for example requiring utilities to increase chemical stockpiles, may

create a range of dangerous goods risks and conflict with jurisdictional level requirements, such as environmental and dangerous goods regulations.

- To illustrate the areas of potential conflict that need to be carefully managed to avoid a perverse outcome for the local community, water utilities in Victoria are covered by the following regulatory/legislative and reporting requirements:
    - Department of Environment, Land, Water and Planning (DELWP) undertakes extensive work in supporting and effectively regulating risk and resilience management for the State, supported by the following regulatory/legislative requirements:
        - Emergency Management Victoria obligations through the Emergency Management Act.
        - Statement of Obligations for each water utility.
        - Victorian Government Risk Management Framework.
        - Victorian Protected Data Security Framework.
        - Industry Accountable Officer declarations.
        - Emergency response frameworks are well established at State and Region level – all adopt All Hazards approach.
        - Department of Premier and Cabinet providing cyber response support.
        - Office of the Victorian Information Commissioner.
        - Environment Protection Authority Act and requirements.
        - Department of Health and Human Services – Water Act.
- Reporting must seek to complement not duplicate or increase the reporting burden on CI water businesses.

There is an existing good practice model that enables enforcement of Federal legislation by State and Territory based entities. This model is the Food Act. An agreement between the State and Territory governments developed via COAG has ensured that the Food Act legislation is implemented by State and Territory health regulators without amendment. Such an approach is recommended for the implementation of the PSO and the cyber security obligations at a State or Territory level for State or Territory based entities such as Water Utilities.

Q16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

Key aspects that need to be a consideration for the sector regulator:

- Co-designed standards and guidelines that will guide the regulation needs to be coordinated through the TISN Sector groups at a national level consultation with States, Territories and jurisdictions.
- The sector regulator should then utilise industry direction to formalise regulated sector guidance. Where the sector regulator differs, this work should still provide direction on regulatory guidance to ensure consistency.

- The regulator must have skills and resources to assist the sector to comply with any obligations.
- A set of minimum standards that are reasonable and proportionate, formulated collaboratively between the regulator and the sector.
- The regulator relationship should aim to be transparent, constructive and recognise that there are security risks that are shared between government and the sector entities.
- Guidance on how entities will be assessed and how the relationship will be managed.
- The process for sharing information.
- How the regulator will support entities during and after a cyber breach/attack.
- Scalability of requirements so that entities have a requirement proportional to the level of risk and capacity to implement.
- Guidance should be provided by the sector regulator in relation to the responsibilities and expectations regarding specific threats that should be addressed by licence holder. Addressing these threats should be the responsibility of the State, Territory or Local Government owner together with the licence holder through engagement with third party providers not, not through direct regulation of the third party.

Q17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

For the water sector a State or Territory based regulator would be best placed to undertake the regulatory role in relation to the PSO and the Cyber Security Obligations. The situation in each State and Territory differs as to who the regulator could be. Each State and Territory will need to nominate the agency they wish to undertake the regulatory function. Noting that this agency may be supported by other entities such as the Office of the Technical Regulator in South Australia or the Department of Environment, Land, Water, and Planning (DELWP) in Victoria.

The advantage of a State or Territory based entity is the close ties with the State or Territory Economic Regulator and that all of these agencies report to the State or Territory Government. Providing a strong governance link between funding approval mechanisms and regulatory requirements. This is particularly relevant since the legislation does not contemplate additional Commonwealth funding for implementation. Having a State or Territory regulator implementing the Federal requirements will avoid fractious divisions on appropriate funding for controls. Once the controls are agreed in principle then the regulator will need to support them by allocation of funding.

At present some States and Territories have multiple security regulators and the division of responsibility between them is unclear. Therefore, if the water sector is to have multiple/tiered (State/Federal) regulators, there must be absolute clarity on the division of responsibility between them and how the sector/entity relates and deals with each.

Q18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

- Detailed understanding of the sector.
- Advisory panels to assist the appointed regulator understand the sector and account for sector context and other regulatory imperatives.
- Clear articulation of the PSO's to ensure consistency in application.
- The emergency management oversight function within the regulator will need additional skills in cyber security, and response co-ordination that leverages existing initiatives such as the Joint Cyber Security Centre. Co-ordination of both cyber response and security obligations must be aligned to streamline reporting obligations rather than create additional overheads.

Q19. How can Government better support critical infrastructure in managing their security risks?

- The articulation of a funding/cost recovery model that recognises and accounts the way the sector is funded, which can support security requirements above and beyond what the market will bear.
- Clearly defined standards, which are appropriate, reasonable and proportionate.
- Two-way communication that is based upon mutual understanding and respect, which recognises that key security risks are shared between the sector and government.
- Critical incident support.
- Security intelligence/situational awareness, this includes threat intelligence, the effectiveness of treatment measures and the provision of a security roadmap to enable forward planning.
- Support for Supply Chain security, particularly given that many water businesses use the same equipment and service providers.
- Creating greater awareness of TISN as the national threat information sharing network.
- Supporting entities with training and tools.
- Assist entities to develop systems and process to comply with obligations and assess maturity.
- Developing clear guidance in relation to the security requirements around the type of information being shared, how it is consolidated and version control.
- It is important that there is consistency in regulatory standards across the sector. Differences in standards and approaches would impose additional costs on third party providers who are active in multiple States and Territories.

Q20. In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

The implementation of such a scheme would need to be proportionate to the risks. In water, the disaggregated nature of the sector and low number (if any) of Systems of National Significance are indicators that such a measure would not be commensurate to the current level of national risk in relation to the water sector. Noting the application of the Personnel Security principles as part of the Positive Security Obligations will provides direction on appropriate personnel security risk controls including vetting. These would then be operationalised with clear guide on best practice for the sector though the sector regulation.

In particular:

- The water sector recognises the benefits of AusCheck scheme.
- The water sector believes that the application of the scheme should be calibrated to or aligned with the graduated or hierarchical classification scheme as advanced in Figure One of Consultation Paper.
- Therefore, the question of whether the water sector should be subject to such a scheme depends upon its eventual classification within that typology.
- If the water sector is subject to this scheme, then the question of which roles should require an AusCheck should be matter of negotiation between the sector, the entity and the regulator.
- The water sector recognises that there are cost and IR impacts inherent in the AusCheck scheme and that this needs to be weighed against its potential personnel security benefit. The current costs of these impacts are uncertain and requires more detail, particularly in relation to how broad (in terms of coverage) would the model be. Should it be applied to employees, contractors or both, and whether existing controls were sufficient to address the perceived threats?

Q21. Do you have any other comments you would like to make regarding the PSO?

The new framework needs to take into account the time and/or financial cost that small or regional water corporations might have to bear in order to meet the security obligations. The level of security standards stipulated in the new security obligations must be carefully considered in terms of cost implications for smaller water corporations that may require additional financial support from Government.

In addition to the response to Question 16 regarding the clarification of responsibilities between water business licence holders and third party operators. As infrastructure operators have entered into commercial agreements with licence holders that have not considered cybersecurity risks, a mechanism to enable contracts to be varied on equitable terms could be beneficial to expedite the implementation of improved cybersecurity performance of critical infrastructure assets.

Where licence holders are tendering new work, it is critical that cybersecurity requirements are considered and clearly specified. This includes the allocation of responsibilities and associated risks. These allocations are likely to differ widely, based on the type of commercial arrangement (for example, between a BOOT and operation of assets without responsibility for their maintenance and renewal).

Enhanced Cyber Obligations

Q22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

Additional areas of assistance would include:

- A national real time information sharing network under TISN to allow rapid sharing of information on emerging threats and quick isolation of threat vectors.
- Education and awareness training to ensure all organisations captured by the enhanced cyber obligations and the Step In powers are aware of not only their obligations but how to effectively prepare, react and interact on threats. Training programs should not be limited to ICT teams.
- Communication - Security intelligence (filtering of intelligence so we cut through the noise and focus on appropriate concerns).
- A clear set of national good practice cyber security guidelines and implementation framework, coupled with a regular cyber security maturity assessment to ensure consistent minimum security levels are achieved and maintained nationally.

Q23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?

- Whilst the focus in the Consultation Paper on situational awareness is a worthy concept, to maintain the necessary level of mutual information sharing will take significant time and effort.
- In addition, any information sharing on situational awareness will need to take into account and build on existing relationships between the Commonwealth and the States, Territories and jurisdictions.
- Situational threat information-relating to sector dependencies, e.g. water is reliant on electricity, if a credible threat to the energy sector is identified the water industry must be advised what level of risk that presents to service provision so we can prepare contingency, ramp up resources or stage equipment at critical assets.
- Pathways and experiences facts on meeting security maturity, advisories and obligations (remove multiple agencies doing the same research, testing, making the same mistakes).
- Cloud services research and alignment.

Q24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

- Cloud services research and alignment.
- Pathways and experiences, facts on meeting security maturity, advisories and obligations (remove multiple agencies doing the same research, testing, making the same mistakes).
- Situational threat information, within sector and relating to sector dependencies,

Q25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

- Good practice cyber security management across the entire organisation in terms of following the Essential 8, and looking to attain compliance against the NIST Cybersecurity Framework or IEC 62443.

- Cyber, Personnel, Physical testing should be carried on a regular basis by the entity and independently on a regular basis. (Pen testing, vulnerability assessments, red teaming, background checking).
- Awareness and training best practice needs to be deployed for any security involving humans.
- Security risk assessment guidance from the CSC to entities to increase understanding of threats and also information from ASIO on any relevant threats of a physical nature.

Q26. What are the barriers to owners and operators acting on information alerts from Government?

The owners of water businesses are State, Territory and Local Government. There needs to be a defined flow of information between the Federal Government and the State, Territory and Local Government owners to ensure smooth engagement and action on relevant alerts. There should not be an instance where the State, Territory or Local Government owners are not kept informed of relevant alerts from the Federal Government.

The information alerts from Federal Government will need to be relevant, specific and preferably outline the level of threat and the proposed actions or countermeasures. If the proposed actions have initially been agreed by the State, Territory or Local government then action is likely to be quick and as per direction. Without effective engagement of the State, Territory or Local Government owner it may be difficult to implement some actions, particularly where these require additional funding, are contradicted by State or Territory legislation, or could adversely impact the business or its customers. It is important that there is a genuine threat associated with an alert to ensure long term credibility and engagement.

Additional barriers are:

- Financial
- Resourcing
- Capability / knowledge
- Technical debt
- Frequent non-relevant external risk alerts
- Expectations of government, regarding the response, particularly for smaller water businesses that have resourcing constraints.

Q27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

The Consultation Paper’s proposal to undertake “preparatory activities” to build understanding and capability of threats could provide valuable means to improve security posture, especially in relation to entities’ maturity in responding to, managing and/or preventing incidents. The playbook deliverable associated with this initiative would provide considerable value to entities’ incident management processes and business continuity planning.

The following are proposed to enhance the value of the playbooks:

- Playbooks should be developed by entities after receiving a common template from the TISN / WSSG / government with a review as part of an external audit periodically.
- The work must recognise and incorporate State and Territory Government jurisdictional “playbooks” and incident processes
- No barriers, it should be clear that we need to work together.
- The playbook should be 90% sector specific with just the ‘personnel’ details being unique.
- This playbook should be built with all sector entities.
- Playbook should include:
    - alignment with standard Information Technology Service Management (ITSM) incident processes - this should not duplicate an organisation’s current incident process
    - contacts and escalations
    - messaging and communications
    - event types
    - business related continuity arrangements; and
    - participate in regular cyber security activities “cyber war games”.

Q28. What safeguards or assurances would you expect to see for information provided to Government?

- A transparent process to ensure that the shared information does not subsequently become a regulatory impost.
- Non-Disclosure of sensitive information.
- Information is used only for SOCI purposes.
- Security commensurate to the level of information classification.
- Ensuring Critical Infrastructure Entity (CIE) are not named and remain anonymous.
- Disposal of information on request of the CIE or in accordance with the appropriate records act requirements.
- Information provided to Government should be validated before it is shared & have a high degree of confidence - however that shouldn't stop information from being shared. Information should come with a confidence rating (Admiralty scale).

Cyber Assistance for entities (step in powers)

Q29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

1) Where the State or Territory Government invites Federal participation through declaration of a State of Disaster or similar.

2) Where the Federal Government becomes aware of a cyber security threat that has or is likely to affect multiple critical infrastructure entities across sectors or State or Territory boundaries. These could include:
   a. When/where a Nation State attack is assessed (with a high degree of confidence) to be imminent and there is a shared understanding/acceptance that:
      - the government has the capability to control, deter or prevent the ongoing threat from being realised; and
      - the sector/entity does not have the capability to control, deter or prevent the ongoing threat from being realised.
   b. In a rapidly escalating geopolitical environment where nation state war is imminent or in progress.

      The actions taken in these circumstances should be proportional to the risk. The actions that are developed should be aimed at ensuring:
      - Continuity of operation for the affected critical infrastructure.
      - That critical infrastructure relied upon by other entities is adequately protected.
      - Optimal co-ordinated of the national effort.
      - Resources and responses are prioritised efficiently both during the event and the recovery phase.

Q30. Who do you think should have the power to declare such an emergency? In making the declaration, who should they receive advice from

At a State or Territory level the power would reside with the Premier, at the Federal level the Prime Minister. In making this declaration advice should be sought from Home Affairs, the First Ministers Office in the relevant State(s) and/or Territory(s) along with the entity concerned.

There must be clarity on the trigger and mechanism for step in powers of the Federal Government and how these interoperate with State, Territory and Local Government legislative obligations and individual water corporation emergency management plans. The risk of impacting Public Safety with any directed actions must be assessed before a declaration is actioned.

Q31. Who should oversee the Government's use of these powers?

Oversight of these powers would be subject to review by Cabinet and subject to judicial review at the request of National Cabinet or through a request from State or Territory First Ministers via the National Reform Council.

Q32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyberattack, do you think there should be different actions for attackers depending on their location?

Location strictly speaking is not relevant – however, in the broad sense this will be a matter for government based upon a range of geopolitical considerations

Q33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

It makes good sense that legal protections would be afforded for these circumstances so that people could act confidently and in a timely manner. Depending on the nature of the directive being given to water infrastructure licence holders the legal protections could include, indemnity from prosecution if the directive is contrary to State, Territory or Commonwealth law and relief from commercial penalties (abatements, etc.).

Protections must accrue to officers and Directors of an entity who are acting under direct instruction or direction from the Federal Government, in accordance with their delegations. These provisions should protect an officer or Director from prosecution through statutory immunity or general immunity, where it can be shown that the actions taken were within delegation and reasonable to address an imminent cyber threat or incident that could significantly impact Australia's economy, security or sovereignty.

Q34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?

Whilst we recognise that the ability to intervene may be appropriate in certain circumstances, additional clarification is required to identify the appropriate triggers for such action, the parameters under which such power may be exercised, the role of the entity during this period, and the implications for all parties arising from such an event.

The use of the powers needs to be subject to review by National Cabinet to ensure that the actions requested were appropriate and proportional. The risk of impacting Public Safety with any directed actions must be assessed before a declaration is actioned.

There needs to be in place a right of appeal to the appropriate use of these powers. This right of appeal should be through the Federal Court.

Q35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

It is the Sector's understanding that the cost benefit analysis for this work has been put together for the Federal government considering the benefits from addressing risks associated with cross sector dependencies. The water sector has had no incidents of national significance in over 120 years of operation. For example, even during the blackout across South Australia in September 2016 where there was significant national cost, there was minimal cost impact on SA Water and no flow on national impact associated with the water supply, and this example of water sector resilience is mirrored across all States and Territories within the "all hazards" risk context.

Costing the benefits of cross sector effects significantly overestimates the benefits to the sector. This approach will cause inequity in the cost allocation between sectors and undue burden on water business customers because of the inability to transfer costs.

In addition, when costing the benefits of managing the risks it is important to apportion the benefit over a number of years, because the frequency for multi-sector events of national significance is low. This is in contrast to the costs, which are an ongoing annual expense.

Further the current costings appear to be flawed because the regulations are not yet defined along with the mechanism(s) to meet the regulatory outcomes. We need the details of the regulation before any accurate costing can be provided. The modelling we have seen includes cascading effects of disruption and that is an inappropriate method for calculating the cost of disruption as indicated above.

Suitable mechanisms for covering costs of incident related response and recovery need to be in place. These vary unsatisfactorily across borders. For example, the NSW Government has the Environmental Trust, which provides a good model for a national fund. In Melbourne, many of the waterways incidents are funded by Melbourne Water out of customer funds, which is not appropriate. There is a need to resolve this for major security-related incidents.

In a situation where Federal Government has to step in, there should be a clear road map on how the incident response will be coordinated amongst the Federal Government, State/Territory/Local Government and Water Corporations, particularly the proportionality of these powers and the overall impact on water corporation’s ability to continue its business operation.

The risks to water utilities depend on the nature of the attack, but can range from environmental harm, to potentially harming large portions of the population, to causing a lack of public confidence in the utility, through to significant economic loss. These risks are constantly monitored and managed by water utilities on a daily basis, as such they are currently well managed through existing risk control mechanisms. Since the formation of entities supplying reticulated water in Australia, there has never been a water security related incident that could not be managed at a State or Territory level or below.

Some of the key cyber risks identified by the sector include:

- Reliance on black box products and services (e.g. pre-packaged computer systems) with common infrastructure (e.g. pumps).
- Cloud-based infrastructure.
- Supply chains (including chemical, equipment and IT) and trust in the products supplied by those supply chains – especially when international.
- Costs would likely increase due to the narrowing of the approved supplier lists.

Separately, a key risk from the Step In powers are that the Federal government representatives may have no or limited understanding of the functions or operation of a water business. Therefore their effectiveness could be quite low. This needs to be addressed through trust and information sharing, along with allowing the option for the Federal government to be supported by trusted experts from within the sector. Such an approach needs to be built over time through TISN.

Sovereign risks are currently posed to the sector are by the current Exposure Draft for the Foreign Investment Reform (Protecting Australia’s National Security) Bill 2020. The concern here is about subcontractors who manage water infrastructure on behalf of the water business licence holders. The risk is of the Treasurer using the proposed Call In powers to make a prohibition or disposal order in relation to a significant third party service provider.

This may reduce innovation by inhibiting engagement with potential foreign, service providers.

However, it has been suggested by Home Affairs that entities contracted by licenced water businesses or form part of the supply chain for licenced water businesses may be captured by the Step In powers. This may cause sovereign risk to these entities who may be completely unaware they are covered by the Step In powers. The cyber risk from these entities falls into two categories: 1) entities directly contracted to run assets owned by the licenced water business and 2) entities involved in supply of goods or services to licenced water businesses. For directly contracted entities, the current arrangements are that they run the digital systems but the water business owns and controls any data associated with instruments or control systems. Therefore, any data risk will occur directly to the licenced water business, not their subcontractors.

Suppliers to the water industry may be impacted by cyber threats. However, the impact to the licenced water business should be addressed through good practice supply chain contingency management. This will be primarily using existing contracting tools, of which the Federal government will have no or very limited awareness. Direct intervention to address supply chain risk is most effectively done through the licenced water business, not by engaging with the supply chain in a crisis situation. Effective contingency planning can avoid such risks. This should be part of the PSO.

For these reasons the water sector believes that the Step In powers should only apply to licenced water businesses, not their subcontractors or supply chain. Including subcontractors or the supply chain creates risk and uncertainty which can be more appropriately managed through the PSO’s and direct engagement via the licenced water business who has the direct contractual relationship. It is the licenced water business who is accountable to the regulator, government and the customers and therefore owns the risk.

Q36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

The key challenge with assessing the appropriateness of this legislation is the uncertainty around the risks. The water industry has not previously required national assistance for any cyber related issue, but the industry accepts that the situation is changing, systems are being more automated and remotely controlled. The probability of and the consequence from a cyber security attack are both increasing. However, it is still not judged a risk likely to require direct Federal Government intervention nor are the consequences likely to be assessed as national or jurisdictional, but will be confined to systems within a water entity. The industry considers direction particularly on the required cyber security standard from the Federal Government should be sufficient to ensure these increased risks can be adequately met.

The proposed model is a response to an evolving geopolitical context and a realisation that the existing regulatory models are no longer fit for purpose. The water sector agrees with this proposition but is keen to ensure that what eventuates involves:

- Proportionate and reasonable sector specific standards (based upon sector agnostic principles) that have been derived through collaboration with the sector.

- The provision of timely, actionable and relevant information and intelligence bespoke to the sector/entity.
- Government (the regulator) recognising that the entity is best placed to assess its own vulnerability and in turn process good intelligence into effective security risk management.
- Intelligence/information collection plans for a sector that have been determined in consultation with the sector, based on the sector risk context.
- The recognition of the sector’s ability (or inability in some cases) to resource proportionate and reasonable security.
- The recognition that key security risks are shared between government and the sector.
- The recognition that some security risks that impact a sector have been generated as a result of government policy (i.e. relations between nations) and that the costs associated with their management would best be met by government.