WATER SERVICES
ASSOCIATION OF AUSTRALIA

WATER INDUSTRY SUBMISSION

Security Legislation Amendment (Critical Infrastructure) Bill 2020 – Exposure Draft
Intelligence Services Regulations 2020

27 November 2020

Attention: Hon Peter Dutton MP
Minister for Home Affairs
PO Box 6022
House of Representatives
Parliament House
Canberra ACT 2600

SUBMISSION: Security Legislation Amendment (Critical Infrastructure) Bill 2020, Exposure Draft and Intelligent Services Regulation 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		[redacted]
Sydney NSW 2000		[redacted]
[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.

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 on 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. Its 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.

1. EXECUTIVE SUMMARY

There are a number of concerns with the exposure draft that are detailed in the following pages. However, the Water Sector wishes to call out the following two areas of highest concern.

1.1 Checks and balances

Whilst we applaud the proposed engagement with the sector and affected entities in developing Positive Security Obligations (PSO's) and Rules there is no formal appeals process for Rules made by the Minister. If the sector or an Entity objects to any proposed Rule the only recourse is an appeal to Parliament. This is an exceptionally high bar for contesting any proposed Rule.

This lack of checks and balances permeates the exposure draft (as outlined in Section 2.4) particularly in the areas of risk management, privileged information, cyber security and Systems of National Significance (SONS). The lack of conventional rights of appeal and oversight erodes natural justice and provides significant concerns in relation to potential regulatory over-reach and poor community outcomes.

To provide the right of appeal and independent review outlined above, the water sector recommends that the *Inspector General of Intelligence & Security* or the *Commonwealth Ombudsman* as suitable agencies to conduct the oversight function for these proposed amendments to the SOCI Act.

1.2 State, Territory and Local Government arrangements

The Exposure draft does not recognise the different governance arrangements across all sectors. Water businesses are owned by, report to, and are funded by, State, Territory or Local Government owners and regulators, with pre-existing regulatory regimes. The exposure draft does not have a clear approach for recognising this fact, nor engaging with these key stakeholders and decision makers. It is vital that State, Territory and jurisdictional owners and economic regulators in particular are directly engaged during the formulation of Rules and PSO's.

There is also a lack of clarity on how resolution will be achieved in cases where there is a disagreement in assessment of the risk and response priority and proportionality of risks. As the overarching risk owner, it is essential that States, Territories and jurisdictions have a formalised and legally supported right of reply on all Federal controls.

2. GENERAL COMMENTS

The Water Sector notes this this is a highly important piece of legislation for critical infrastructure (CI) sectors. However, the exposure draft response period is manifestly insufficient for a comprehensive submission and directly brings into question the Commonwealths statements on meaningful collaboration with industry.

The exposure draft in its present form represents a clear philosophical change of direction from the *Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act)*. It seeks to broaden the scope from 'national security' to the management of CI risk more generally. It has also adopted an adversarial 'look and feel'. This is regrettable given that government and CI entities have had a long history of cooperative engagement aimed at sharing the risk.

We understand government's desire to ensure that CI is adequately protected and that its risk management arrangements are 'fit for purpose'. This is particularly the case given the dynamic geopolitical environment in which we find ourselves; and the strong nexus between the health of the Australian economy, the security and wellbeing of the community and the resilience of CI. However, we would have preferred the exposure draft to clearly define the relationship between government and industry as a partnership based on mutual collaboration. The Government could address this by amending Part 1, Section 3 of the SOCI Act to highlight cooperation and collaboration, with the SOCI Act's compulsions and penalties to be imposed as a last resort.

The overall approach being taken is more akin to how environmental, safety and emergency risk is regulated at the State or Territory level, which we argue is not translatable to protective security because of their vastly different control architectures. Successful protective security depends upon the close cooperation of intelligence and law enforcement agencies and the CI sectors, the goal of which is to achieve a common understanding of threat and its bearing on security posture. The attainment of this 'shared understanding' is a precursor to the successful management of a distributed risk, which we argue is not given sufficient emphasis in the exposure draft.

All large mature water businesses overtly captured by the SOCI Act are acutely aware of their business risks. These are reported regularly to the Board Committees and Board of the water entity and the jurisdictional government owners of the water entities, which is a conventional and proven mechanism for the successful management of enterprise risk in a corporate setting. The ingredient that is most often lacking in the corporate security risk management equation is high quality threat data, which only government can provide. Unfortunately, the exposure draft in its present form does not give sufficient weight to this, conveying instead the impression that this is not the prime intent of the legislation. We trust that the situation will be different in execution and that the provision of advice and intelligence will be captured in the concomitant regulations, rules and standards.

Intelligence Services Regulations 2020: The water sector also notes with concern the proposed change to the *Intelligence Services Regulations 2020*, which formally removes any suggestion of confidentiality with the support provided by the *Australian Signals Directorate (ASD)* and the *Australian Cyber Security Centre (ACSC)* to industry and negates the applicability of the ASD-ACSC confidentiality agreements.

2.1 Perceived Intent

We believe that a fundamental intent of the legislation is to give government the head of power to mobilise and defend CI if Australia's strategic situation rapidly deteriorated or a deeply serious cyber-security event occurred. This is entirely appropriate if you look at the CI security challenge as it may be shaped by increased international uncertainty and strategic competition. However, the exposure bill grants extraordinary powers to government in situations well short of unconstrained international competition or conflict. Consequently, there is a need for proportionality along with appropriate checks and balances to be 'baked into' the legislation. We feel that this is not the case at present but having been granted these powers through legislation, we must depend solely upon the sound judgement and good intent of government to ensure abuses and overreach do not occur.

The sector questions the objective and need for the rush to pass this legislation and suggests that this may result in ineffective outcomes. The timing prevents industry having any meaningful right of reply to guide changes to the legislation to make it more effective for both industry and government. If the intent of the legislation as called out in the Explanatory Memorandum is to build trusted partnerships between government and industry to manage and minimise security risk, then more time should be taken to get this right through those partnerships. Time taken with this would likely in turn expedite the development of sector specific Rules and Regulations and ensure more effective outcomes

2.2 Role of Bill

Regulatory action, such as Step In powers are extreme measures and it should be made clear that they are only exercisable for the most extreme and pressing circumstances (e.g. major conflict or a build-up to same).

2.3 Trust Building and Collaboration

The SOCI Act and Exposure Draft are currently geared for the flow and collection of information to be a one-way provision, from each CI entity to Home Affairs. This provides the Critical Infrastructure Centre (CIC) with great situational awareness and organisational intelligence. It would be highly beneficial to encode two way sharing of this information through the TISN in the interests of enhancing shared situational awareness to support national security and resilience. States, Territories and jurisdictions would be able to better regulate and manage their CI if they are provided up to date information from the Commonwealth,

The Bill permits intervention prior to a Cyber Security Incident based on Ministerial authorisation. This means we can have an intervention order prior to an event without our involvement or knowledge in that event. There needs to be controls in place that allow us to work with the CIC prior to an intervention, and that intervention should only be used where the entity is not co-operating or lacks the capability to respond. This is especially important for Systems of National Significance (SONS) where the entity is required to have a relationship with the CIC. A positive relationship should not include use of Step In powers without agreement.

The proposed change to the *Intelligence Services Regulations 2020* further compromises the confidential sharing of information between the CI Entity when seeking positive support from the ASD (ACSC).

2.4 Right of Appeal/ Appropriate Checks and Balances

Whilst we applaud the proposed engagement with the sector and affected entities in developing PSO's and Rules there is no formal appeals process for Rules made by the Minister. If the sector or an Entity, or a water Entity jurisdictional owner or water business regulator objects to any proposed Rule the only recourse is an appeal to Parliament. This is an exceptionally high bar for contesting any proposed Rule. In addition, the sector is also concerned that there is also no formalised requirement for any cost benefit analysis to be conducted before implementation of a new Rule, leading to a manifest risk of disproportionate compliance obligations.

2.4.1 Risk Management

Section 30AH effectively undermines the sovereignty of every CI owner – it allows the HA Minister to direct the business to address or minimise any risk – perceived or real, that the Minister deems appropriate, without justification, a Regulatory Impact Statement or right of appeal, if the Minister is satisfied of an imminent threat or that a hazard has or will have a significant impact on a CI Asset. Otherwise there is a 14 day public and First Ministers consultation phase. However, there is no right of appeal if the outcome is not considered good practice by the CI owner. Note also that any such requirements to not need to be consistent with or consider licence conditions or any other State/Territory or jurisdictional legislative obligation or pre-existing agreed infrastructure program priorities. The only protection is that the final Rule must be tabled in Federal Parliament.

The notes to the Bill and the consultation process indicate that existing risk management processes will be taken into account. However, the process by which existing programs will be assessed is unclear. The sector is concerned that if current processes are not deemed adequate or appropriate then any 'critical infrastructure risk management program' could increase costs without measurable or material benefit to the Entity's asset risk profile, but without any right of appeal other than to Parliament.

2.4.2 Privileged Information

The requirements under sections 30DG(2), 30DN(2) and 35AN(2) could lead to abuses of power by the agency administering the SOCI Act, particularly as the Entity to which the privileged information is handed has regulatory powers to penalise, take action against or Step In and operate. These provisions are inconsistent with other Australian regulatory regimes and the procedural right to obtain open and frank legal advice that is and remains confidential.

A water business should be able to obtain legally privileged advice which is not waived in order to protect customers, protect itself, ensure there are no contractual breaches under existing contracts, understand its obligations (under both the SOCI Act and third party

contracts), to assess requirements for compliance with the SOCI Act (including abuses of power) and to receive advice about the validity of any regulatory action and possible defences. These new provisions are overstepping a regulator's role. A party should be entitled to the privilege of confidential legal advice in a manner that protects the entity to mitigate abuses of power by a regulator.

Further, Section 30DG undermines common law defence of privilege against self-incrimination – i.e. that a person is excused from providing evidence on the grounds it may incriminate them. Where is the legal recourse and review of requests from the Secretary to ensure the request or refusal is reasonable?

2.4.3 Cyber Security

In the cyber security arena, Section 30DJ the legislation allows HA to install software with impunity from liability and any damage to the Entity's systems (although it must be in consultation). There needs to be some right of appeal or ability for the Entity to recover costs, share responsibility or to seek appropriate restitution if damage is done, regulatory service obligations are breached or other losses incurred, by these enforced Commonwealth actions.

2.4.4 Declaration of a System of National Significance (SONS)

The definition of a System of National Significance is broad, without balance, and there are no provisions within the Bill for Regulated Critical Infrastructure Entities declared a system of national significance to seek a review of the declaration or to overturn the declaration, despite the significant additional regulatory burden imposed on owners and operators of a system of national significance. Without an appeal mechanism, the owners and operators of a System of National Significance could face significant operational and compliance costs without access to natural justice remedies.

The water sector notes the preliminary verbal advice that water entities are unlikely to be declared *Systems of National Significance*, however the water sector also notes that this preliminary verbal advice is unsupported by legislation. A review of the water sector, demonstrates that there are no water entities whose 'systems' and assets cross geographic boundaries, and that they are all wholly owned and responsible to only jurisdictional State, Territory or Local Governments, and therefore by definition cannot be defined as *'nationally significant'*

2.4.5 Proposed solution

To provide the right of appeal and independent review outlined above the water sector recommends that the Inspector General of Intelligence & Security or the Commonwealth Ombudsman as suitable agencies to conduct the oversight function for these proposed additions to the SOCI Act.

2.5 Confidentiality

The water sector has concerns about the conflict/mismatch between having to maintain confidentiality versus seeking costs for implementation through State or Territory Regulators,

and owners. The current mechanism allowed through the SOCI Act is that the Entity cannot directly disclose CI obligations to their State or Territory Economic Regulator if they were to be declared a System of National Significance or are operating under Direction from the Minister for Home Affairs in respect of the SOCI Act. This constraint applies even for the purposes of seeking funds to implement Commonwealth requirements under the SOCI Act. If a water utility is unable to explain the reason for additional costs is has incurred, for example by complying with regulations, it is unlikely to be able to recover these costs through current pricing mechanisms with State and Territory regulators and their owners.

Under Section 42 of the SOCI Act, the Secretary can disclose this information to the State, Territory Minister or local government representative with regulatory oversight of the Entity, or their staff. However, direct disclosure between the Entity and their regulator has not been enabled. This presents a highly inefficient process for financial approval of Commonwealth requirements under the SOCI Act, which could result in sub-optimal and potentially perverse outcomes for the Entity and the Community. The SOCI Act needs to be amended so that the Entity is able to directly engage with their State or Territory economic regulator for recovery of costs in relation to implementation of requirements under the SOCI Act.

Similar conflicts may arise with respect to contracting when seeking a variation or upgrade arising from a direction or requirement imposed under the SOCI Act. The contractor usually needs to understand the reason for having to implement the change in order to most effectively mitigate risk and manage costs, particularly on large scale projects. A failure to consider this requirement will lead to increased costs for the water business and its customers.

2.6 State, Territory and Local Government interactions

2.6.1 Owners and regulators

It is disappointing to see that the previous submission recommendations in relation to State, Territory and Local Government, owners and regulators don't appear to have been considered in developing the Exposure Draft.

a. When the *switch on* powers are activated, there needs to be strong engagement with not just the entity or sector, but also their owners and regulators. It is vital the SOCI Act needs to explicitly enable engagement with not only the Entity but also require the Commonwealth to engage with relevant State, Territory or Local Government Owners.

b. The Bill gives Home Affairs the ability to engage directly with an Entity's Board without engaging the owner. The Bill must be amended to require engagement with the relevant State, Territory or Local Government Owner prior to engaging the Entity's Board.

2.6.2 Incident Management and Enforcement Agencies

There are already jurisdictional agencies overseeing security of infrastructure in each State and Territory (e.g. the police, CyberNSW, Department of Environment, Water, Land and Planning in Victoria). It is unclear how the different regulators will work together and whether

the SOCI Act will put undue pressure on some State, Territory and jurisdictional based Entities to perform to two separate requirements (State and Federal), and how conflicts or inconsistencies will be managed to the extent they exist. Note also that many water business contracts include existing State, Territory or Local Government requirements and so may not deal with the new SOCI requirements to the extent they differ or impose new security obligations.

The sector typically manages incidents through existing State, Territory or Local Government mechanisms, which are generally aligned to the nationally recognised Australasian Inter-Service Incident Management Systems (AIIMS). The SOCI Act should explicitly recognise that where existing measures are in place for the sector that these will be recognised to the extent possible.

During a State or Territory wide incident, where the Commonwealth determines it needs to use the Step In Powers, there is no clarity in the exposure draft on who is the lead agency where there are existing State or Territory based jurisdictional controls for incident management already in place. The Exposure Draft is silent on this area, which has significant potential for misunderstanding, confusion, duplication of reporting and negative outcomes. The legislation needs to provide the ability to recognise existing State or Territory based agencies and structures whilst supporting their authority to lead and respond to current and emerging situations. Reporting and Report Timing

2.6.3 Annual Reporting

Section 30AG obliges regulated participants to report on the program annually. While this is a reasonable transparency requirement, this report must be provided within 30 days after the end of the financial year and signed individually by each member of the regulated participant's board or similar governing body. These requirements are overly prescriptive, and inconsistent with normal corporate governance practice. Most regulated participants already have an existing corporate risk oversight and annual report endorsement arrangement in place and compliance with the Bill should be incorporated into these arrangements. Typically existing end of year reporting arrangements are finalised by September of each year. As such, we request that the timing for Board sign off of risk management plans is either changed to 'Annually, as agreed with each Sector' or 'by end of October each year'.

Section 30AG(2)(f) requires that the report is signed off by each member of the Board. The water sector recommends that this is inconsistent with longstanding corporate practices and it would be more consistent with usual governance practice for the report to be signed by 'a', rather than 'all', directors of an entity. The Sector considers an approach such as used in Section 13(2) of the Modern Slavery Act 2018 (Cth) would provide a similar level of assurance through a more practical approach.

2.6.4 Cyber incidents

Reporting a Critical Cyber Incident within 12 hours may not feasible. Often forensics is required to determine the impact. While the explanatory note states, *'In light of this, the obligation to report within 12 hours is only enlivened when the responsible entity becomes*

aware that the incident meets the above criteria', this caveat should now formally appear in the Bill.

Section 30BD requires Regulated Critical Infrastructure Entities to report all other cyber-security incidents that are occurring or have occurred within 24hrs, regardless of the potential significance. Without appropriate clarification, this duplicates existing State, Territory and Local Government owners reporting obligations, and risks creating an onerous reporting regime for industry, with penalty provisions equal to that of a critical incident. The water sector recommends that the Bill clarify risks that need reporting and constrains them to only significant risks, consistent with current State and Territory reporting requirements, and further recommends that as State, Territory or Local Government owned entities, that a State/Territory regulatory or State/Territory oversight agency is able to report *'on behalf of'* a water entity.

In addition, there is no direct cost benefit associated with the 24-hour reporting obligation. This obligation poses additional regulatory burden on entities, particularly over weekends and holiday periods. The US National Institute for Standards and Technology (NIST) 800-53 Standard notes a requirement for reporting within 72 hours, indicating a misalignment with Home Affairs regulatory standards and international good practice. The Sector considers that a 72 hour reporting obligation for non-critical incidents, consistent with international good practice, would be more appropriate.

2.6.5 Implementation Grace Period

Paragraph 264 of the Explanatory Document to the Draft Bill states that entities will have six months to comply with their reporting obligations once their obligations commence. Particularly if the 'critical infrastructure risk management program' requirements necessitate material changes to an entity's risk management framework and practices (for example, policies, procedures, business approaches and reporting requirements). It is anticipated that Rules will also require approval and engagement with State, Territory and Jurisdictional Regulators and Business Owners, and capital funding approval processes, which overlap State, Territory and Local Government budget approval periods, followed by the period of implementation. In addition, some transitions may take a number of years to fully implement. The water sector recommends that Home Affairs amend the requirement to the business having *'an agreed implementation timeline'* with the Department within 6 months of an obligation being declared.

2.7 Risk Management Programs

Part 2A of the Draft Bill, relation to relating to 'critical infrastructure risk management programs', uses terminology inconsistent with international good practice, which is embodied in ISO31000. It is vital that the terminology aligns with ISO 31000 to avoid duplication of work and ensure a clear and consistent approach is adopted.

When preparing the critical infrastructure risk management program, Regulated Critical Infrastructure Entities are required to *'identify each hazard where there is a material risk that the occurrence of the hazard could have a material impact on the asset'.* The terms *'material hazard'* and *'relevant impact'* are not defined in the Bill. While Home Affairs intends to define

the terms in subsequent sector-specific regulations or rules, the uncertainty created by the obligations undermines industry's capacity to assess potential compliance costs. In addition the explanatory document uses the term *'material hazard'* but only the terms *'hazard'* and *'material risk'* appear in the Bill, again creating uncertainty. We also note that the bill fails to use standard, internationally agreed, risk management terminology *(threat, risk, likelihood and consequence),* creating further potential for confusion within and between sectors.

The water sector recommends that Home Affairs include a definition of *'material hazard,' 'material risk'* and *'relevant impact'* in the Bill. While supportive of sector specific rule-making, the water sector recommends that Home Affairs include the clarification that individual businesses can determine for themselves what constitutes a *'material hazard,' 'material risk'* and *'relevant impact,'* as outlined in the explanatory document. The water sector also recommends the bill incorporate standard international risk management terminology where appropriate consistent with AS/NZS 4360 or ISO 31000.

For example, section 30AH(1) of the Draft Bill states that a *'critical infrastructure risk management program'* has a purpose of minimising or eliminating any material risk of a hazard occurring so far as it is reasonably possible to do so. The water sector considers it would be more helpful to use the widely-recognised formulation that risks should be eliminated so far as is reasonably practicable and, if it is not practicable to eliminate risks, to minimise those risks so far as is reasonably practicable. A definition of *'reasonably practicable'* should be provided, as is done in other similar State or Territory based legislation e.g. section 17 of the Work Health and Safety Act 2011 (Qld).

The water sector also considers that due attention should be given to risk 'outcomes' rather than to 'hazards to the asset'. An 'outcomes' approach can best accommodate an entity's resilience and redundancy provisions that are integral to managing risk.

The Water sector also notes that the proposed Commonwealth risk management process compliance requirement, measurably overreaches the pre-existing principles and outcomes based water sector licensing processes, where long standing community established service delivery standards are given primacy, which intuitively implies, and practically requires, that active *'all hazards'* risk management processes are already implemented to support the 'licensed' service delivery outcomes.

2.8 Definitions

Many critical terms in the SOCI Act are undefined or very broadly drafted. This makes it difficult to assess costs and risks for an organisation, until such time as concomitant rules are determined and published. Some of the terms capture operational issues that we believe sit outside the remit of the Bill (e.g. a hazard could be a bushfire). It may lead to either an overly cautious, unnecessary and expensive implementation of security requirements (at customers or taxpayers' costs) or inadvertent non-compliances leading to misunderstandings and unnecessary enforcement and action. Further, given a party may be penalised for non-compliances, the terms should be clear and precise, so a party understands what it needs to do to comply. The terms should not be so unclear as to drive inefficiencies in business and/or take away opportunities to perform functions of the business in a sound commercial manner.

For specificity, the following critical terms lack clear definition:

a. The meaning of ‘hazard’ – this is a term more often used in the safety space, which in the context of the exposure draft could mean anything (e.g. bushfires and other matters that go to operational rather than cyber security issues).
b. The meaning of ‘material’.
c. The meaning of ‘relevant impact’.
d. The meaning of ‘cyber security incident’ – particularly how this is made consonant with existing reporting to ACSC or similar State/Territory based entities.
e. Critical Cyber Security Incident.
f. The meaning of ‘critical infrastructure risk management program’.
g. The meaning of ‘vulnerability assessment’.
h. The requirement for annual reporting – most water businesses already prepare an annual report. Can an approach be adopted that requires a comment be included in an entities’ annual report to release it from the administrative burdens and costs imposed by creating a separate annual report.
i. The use of the term, ‘The Systems’ is unclear and should be defined.

2.9 Civil Penalties

Section 30AG states that failure to comply with the reporting requirements has a penalty of 150 penalty units. This appears inconsistent with other failure to report penalties within the Bill of 50 penalty units. The Water Sector recommends that the Bill be amended reducing the failure to report annually penalty to 50 penalty units.