sunwater

Sunwater Submission to the PJCIS Review of the Security of Critical Infrastructure Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Sunwater Ltd (Sunwater) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in respect of the *Security of Critical Infrastructure Legislation Amendments (Critical Infrastructure) Protection Bill 2022* (Cth) (Bill) seeking to amend the *Security of Critical Infrastructure Act 2018* (Cth) (Act). Please note that this submission represents the views of Sunwater only and must not be taken to reflect a whole of Queensland Government position, or the views of other Queensland Government Owned Corporations.

Sunwater has participated in the consultation process being run by the Department of Home Affairs, including via the Water Services Sector Group under the TISN framework, and generally feels that feedback has been taken into consideration. Sunwater did not individually provide a submission on the exposure draft to the Bill but notes that a submission was made by the Water Services Sector Group/Water Services Association of Australia. Sunwater supports the strengthening of the critical infrastructure sectors and the intent of the Bill, however we wish to raise the following key issues with the latest version of the Bill.

1. Key comments and recommendation

We consider that there are key issues in the current drafting of the Bill that have unintended ramifications for entities (including water entities like Sunwater) complying with the Bill. These key issues would create material compliance difficulties and practical inefficiencies in the operation of Australia's critical assets. Each key issue is summarised here:

- Use and disclosure of '*protected information*' – the proposed section 43E over-regulates the use and disclosure of '*protected information*' by requiring Secretary consent for almost all documents and information falling within the '*protected information*' definition. This would have a significant impact on both asset operation and the information provided to the Minister by entities in addition to causing significant strain on the Secretary's role.
- Reference to relevant documents and standards – the currently proposed Bill drafting in sections 30AN and 30ANA would require compliance with versions of documents or standards that are applied, adopted or incorporated into rules as those documents and standards are updated from time to time. This would potentially require frequent amendments to risk management programs, causing additional cost and operation disruption, without necessarily contributing to the purposes of the Act. Updates to relevant documents or standards should be considered on a case-by-case basis to determine the impact and appropriateness of those changes, including the time and cost to implement those changes as proportional to the security benefits. This would be to determine whether the rules should be updated to require compliance with the updated document or standard. Additionally, a grace period (with public consultation) for implementation of any required changes should be introduced in the Bill drafting.
- Background checks – we are concerned that the reference to the AusCheck scheme in section 30AH(4) unduly limits the manner in which personnel risk and background checks can be undertaken by responsibly entities. This would create operational difficulties, due to the limited information provided in the outcome of an AusCheck process.

In regard to those key issues, we respectfully offer the comments and recommendations detailed below to the PCJIS in respect of those issued identified with the current drafting of the Bill.

2. Protected Information

(a) Comments

The use and disclosure of '*protected information'* by the entity to which the information relates is, under the current Act, excluded from the offences in section 45 of the Act by the operation of section 46(4)(b). The current exposure draft of the Bill proposes to repeal this section and instead replace it with the rights to use and disclose outlined in the proposed section 43E. This is of concern, as the proposed disclosure mechanisms in section 43E are impractical and would significantly impact upon the ordinary operation of Australia's critical assets.

It is an offence under section 45 if an entity "*makes a record of, discloses or otherwise uses*" protected information. Section 46(4)(b) currently excludes application of this offence if "*the entity is the entity to whom the protected information relates*".

Section 43E permits entities to whom the '*protected information*' relates to disclose the '*protected information*' to:

- various Ministers or Government personnel (section 43E(1));
- with the consent of the Secretary (section 43E(2)) for any documents or information covered by paragraphs (b) to (bl) of the definition of protected information or paragraph (c) of that definition so far as it relates to those paragraphs, which includes almost all '*protected information*'; and
- more broadly to '*protected information*' other than the information to which 43E(2) applies (section 43E(3)).

Section 43E does not permit an entity to use this information in any way (or to make a record of it). In the absence of this right, the wording in section 45 makes it an offence for an entity to use or make a record of any protected information related to its operations. This cannot have been the intention, and resolving this drafting issue is imperative to workable legislation.

Further, even as regards to disclosure, the drafting of clause 43E is impractical. The proposed drafting of section 43E(2) is very broad and captures almost all '*protected information'*. Conversely, section 43E(3) is unhelpfully narrow in its application (given it is the inverse of 43E(2).

The broad definition of '*protected information'*, is appropriate in the context of the use and disclosure of such information by third parties (including the Australian Government). However, the impact of this broad definition, coupled with the drafting in section 43E(2) and (3), means that consent of the Secretary would be required to disclose information that would otherwise ordinarily be considered confidential operational information of the entity.

By way of example only, the definition of *'protected information'* includes "*a document or information that .. (bc) is, or is included in, a critical infrastructure risk management program that is adopted by an entity in compliance with section 30AC*". This document and the information contained in it may not be disclosed by an entity to any third party without the consent of the Secretary.

The practical implications for this would include:

- crippling the managerial operation of Australia's critical assets due to burdensome consent requirements on information core to the asset;
- introducing regulatory strain on the Secretary in considering numerous consent requests; and
- threatening the quality of disclosures or documents provided to the Minister (including critical infrastructure risk management programs) due to the risk of burdensome restrictions being placed on use of information needed for operational purposes.

We further note that this proposed change, in effect, would make it more difficult for an entity to use information about their own operations than a third party acting under the entity's implied or express consent (as permitted in section 46(4)(c)). This clearly demonstrates that the proposed drafting fails to accommodate for ordinary and operational use of information in achieving information security.

(b) Recommendations

The simplest and most effective solution to the issues we outline above is that the proposed repeal of section 46(4)(b) and introduction of section 43E be removed from the Bill. Given the existing exception under section 46(4)(b) of the Act is for use of '*protected information'* by the entity said information relates to, the exception allows sufficient protection for an entity to act in its own self-interest of maintaining security without the burdensome and over-regulation of obtaining Secretarial consent.

If the approach proposed in section 43E is to be retained, at minimum, we recommend that the drafting of the proposed section 43E be reviewed to only require Secretary consent to disclosure of the most sensitive of protected information and to clearly include a broad right to use and make record of the '*protected information*' in section 43E. **For example:**

- expanding section 43E to include a broad right to use and make record of all protected information; and
- the proposed section 43E(2) (a disclosure which requires Secretarial consent) be limited to information such as the declaration of an entity as a SONS with section 43E(3) could be expanded to cover all other '*protected information*'.

3. Reference Materials for Critical Infrastructure Risk Management Planning

(a) Comments

The proposed sections 30AN and 30ANA would permit rules made by the Minister for the purposes of section 30AH or 30AKA to apply, adopt or incorporate a standard or a relevant document as in force or existing from time to time. Sunwater agrees that reference to external standards and industry documentation is an effective manner of reducing regulatory duplication while maintaining current-best practice. This can be achieved by referencing those documents and standards as in force at the date of the rules or the date they are applied, adopted or incorporated into the rules.

When updates to relevant documents or standards are released, the Department can then consider the nature of the changes, whether those changes are necessary to achieve the purposes of the Act, the cost and time for implementation of those changes (including by reference to when changes were last made to those rules). Updates to the rules to reflect the latest version should only occur when the cost benefit analysis justifies it, and should be coupled with a reasonable grace period in which those changes need to be made.

As noted in the Bill exposure draft, such documents are regularly reviewed and updated to keep pace with emerging technology, risks, threats and other factors. However, a risk assessment will be made by mature entities to determine the cost benefit of, and the timing for, implementation of those changes so as to mitigate the risk and disruption to operations. The current drafting of the Bill expressly overrides subsection 14(2) of the *Legislation Act 2003* (Cth) which is intended to provide clarity and protection from this type of change in laws. As currently proposed, the Bill anticipates that there would be an automatic and immediate requirement to have regard to the latest version of any document or standard referenced in the rules, irrespective of the applicability, cost or timeframe required to adopt those changes.

(b) Recommendations

We recommend that sections 30AN and 30ANA be amended to:

(i) delete the exclusion of subsection 14(2) of the *Legislation Act* 2003 and delete the wording "as in force or existing from time to time";

(ii) ensure any reference to a document or standard in the rules must refer to the version of that document or standard, and permit compliance with a later version; and

(iii) make express reference to section 30AL to ensure that the Minister is required undertake a public consultation where a document or standard referred to in rules is to be updated, replaced or removed.

Additionally, consideration will need to be given to the accessibility of any documents or standards referred to in rules and how a point-in-time version of that document and standard will be made readily available for entities required to comply with the rules.

4. Background checks

(a) Express reference to AusCheck scheme

The proposed section 30AH(4) provides the Minister the power to create rules that may require that a critical infrastructure risk program include a provision that permits a background check be conducted under the AusCheck scheme and mandating the assessment of information by reference to the *AusCheck Act 2007* (Cth).

The references to the AusCheck scheme in the Bill's drafting would effectively establish AusCheck as the default mechanism for meeting any background check requirement. This is in comparison to any overarching background check standards or other compliant background check schemes that may be included in rules, which are not expressly addressed in the drafting. There is a risk that this would result in risk management programs being required to permit use of the AusCheck scheme, while the overarching standards for a background check scheme (which AusCheck scheme would meet) remain underdeveloped in favour of an AusCheck acting as the 'default' compliance mechanism.

Based on our understanding, the AusCheck scheme has a lower practical utility compared to other methods that may be used for undertaking background checks. This is due to the limited information given in the outcome of a AusCheck background check in contrast to other schemes and/or processes. For example, the AusCheck scheme provides a "pass/fail" background check. Other methods may provide details of potential issues and allows the entity to assess the associated risk of any issue identified against other operational factors (such as shortage of skilled resources in regional areas in the context of minor historical indiscretions). If the AusCheck scheme were to act as a 'default' under rules for risk management programs it would reduce the information available to entities and reduce the entities ability to assess and manage any perceived risk or create unnecessary duplication in the background check process if the entity still has to undertake its own operational process to obtain further information.

We acknowledge that the inclusion of section 30AH(5) ensures that any rules in relation to background checks and applicable standards are not inherently limited to the AusCheck scheme, and that it would remain open for the Minister to make standards permitting background checks by means other than the AusCheck scheme. However, the proposed drafting in section 30AH clearly sets AusCheck up as the default mechanism in preparation of future rules.

(b) Recommendations

Given the practical limitations of the AusCheck scheme, we recommend that further consideration be given to the drafting in section 30AH to ensure it is clear that:

(i) rules made for the purposes of section 30AH(1)(c) may require a critical infrastructure risk management program include provisions permitting background checks be conducted and the types of background check that may be required for certain types of critical infrastructure, without expressly limiting this to the AusCheck scheme; and

(ii) permitting of a background check through the AusCheck scheme in a risk management program does not limit the ability of entities to undertake background checks to assess the types of information comparable to that assessed by the AusCheck scheme.

5. Concluding comments

We welcome the opportunity to further engage with the PJCIS and Australian Government on these important issues and further explore our perspective the recommendations proposed for addressing the outstanding issues in the Bill in the future. We consider such consultation and discussions paramount in ensuring the reforms proposed in the Bill balance the objects of the Bill with the practical considerations necessary for operating Australia's critical assets.