Australian Government
Department of Home Affairs

# Department of Home Affairs supplementary submission to the Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

## Parliamentary Joint Committee on Intelligence and Security

9 March 2022

# Table of Contents

# Supplementary Submission

1. The Department of Home Affairs (the Department) welcomes the opportunity to make a supplementary submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee's) review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the Bill).
2. The Committee published 45 submissions on their website as of 7 March 2022, of which 23 entities also provided submissions to the exposure draft version of the Bill. In this submission, the Department will address the key recommendations, concerns and suggestions raised by stakeholders in their submissions to this review.
3. This submission addresses matters raised by stakeholders in their submissions to the Committee, and this submission seeks to provide further information to support the Committee in its review of the Bill.

## Consultation

4. The Committee has called on submitters to provide views on the approach that the Department has taken in relation to consultation on the Bill and whether stakeholders believed that their feedback had been incorporated in the Bill or addressed in explanatory material.
5. The Department notes that various submissions supported the efforts of the Department and viewed the consultations as thorough, detailed and constructive. Other submissions raised concerns to the timing of the consultation period and that it was too short to fully consider the issues raised.
6. Extensive consultation has been a cornerstone of the reforms to date. The Department's first submission to this inquiry outlined in detail the extensive consultation on the exposure draft of the Bill, including four industry town halls from 21 December 2021 through to 4 February 2022. During this period, the Department supported the Minister for Home Affairs (the Minister) to hold nine sector-specific roundtable meetings with senior executive representatives from critical infrastructure sectors to ensure the intent of the reforms was understood and supported at the highest levels of industry. The roundtables also proposed a number of amendments to the Bill that the Government took on board.
7. Of particular relevance to this Bill, the Department also engaged extensively on the draft risk management program rules, from March 2021 through to February 2022 – outlined in detail in our first submission. This has consisted of town halls, workshops, multi-lateral and bilateral discussions. As at 3 March 2022, the Department had also received 84 costing submissions from responsible entities to assist in developing a Regulation Impact Statement (RIS) assessing the regulatory impact of the rules.
8. The Department has responded to calls for additional guidance material on the Bill. As with the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act 2021), the Department has prepared a suite of factsheets on each of the obligations in the Bill which will be published on the Cyber and Infrastructure Security Centre (CISC) website upon passage of the Bill. These factsheets will be supplemented by additional **detailed** guidance material, developed with industry, on all proposed and current aspects of the *Security of Critical Infrastructure Act 2018* (the Act). The Department recognises that engagement and education will be crucial to the success of these reforms and is committed to working with entities to ensure these reforms are understood and can be practically implemented. Mechanisms like the Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) are important forums for cross-sector dialogue, and will be key in the Department's ongoing dialogue with industry.

# Regulatory impact

## Regulatory impact analysis

9. The Department notes that many submissions raised concerns with the cost to industry for compliance with both the critical infrastructure risk management program obligations and the enhanced cyber security obligations for systems of national significance (SoNS). Specifically, concerns were raised that the Government had not undertaken—or had not adequately undertaken—an assessment on the costs to industry for implementation of the Bill and proposed legislative instruments.

10. As explained in the first submission to this inquiry, the Department completed a Regulatory Impact Analysis on all of the measures proposed to be introduced in this Bill – apart from the proposed *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022* (risk management program rules) - through its regulatory impact statement (RIS) for the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (SLACI Bill 2020). The Office of Best Practice Regulation determined that no additional RIS was required for the Bill as there was no change to the expected regulatory impact – the amendments to the provisions of the Bill from their original formulation in the Security Legislation Amendment (Critical Infrastructure) Bill 2020 did not affect their cost.

11. Between June 2021 and January 2022, the Department undertook extensive consultation on the development of a draft RIS on the risk management program rules.

12. Both the 2020 RIS and the draft RIS to the risk management program rules identified that implementation of these measures was likely to have the highest overall net benefit of the options explored, including status quo. A clear uplift in all hazards mitigation standards across critical infrastructure, particularly SoNS, will provide the Government, industry and consumers with greater confidence in the resilience of Australia's critical infrastructure providers and the essential services they rely on. Details of the RIS for the risk management program rules is outlined at paragraphs 228 to 233 of the Bill's Explanatory Memorandum.

## Regulatory duplication and existing frameworks

13. The Department notes that submissions raised concerns around apparent inconsistency or overlap with existing legislative and regulatory frameworks. The Department reiterates the point made in previous submissions to this Committee that the Department has worked closely with sectors since August 2020 to identify and avoid duplicating obligations on entities in cases where a class of assets is already subject to a regulatory regime that comprehensively addresses the same outcomes as this legislation.

14. The Bill embeds the need to mitigate regulatory duplication throughout the regime by, for example, requiring the Minister to consult with industry on the introduction of Rules (s 30AL) and by implementing the Positive Security Obligation on an asset-basis by 'switching on' obligations (s 30AB). The Bill reflects industry's view that the reforms should minimise regulatory duplication and will continue to engage with entities to identify and mitigate areas of regulatory duplication.

15. When the Minister specifies requirements in rules made for the purpose of the risk management program, the Minister is obliged to consider existing regulatory systems of the Commonwealth, a state or a territory that imposes obligations on responsible entities. The Minister for Home Affairs has already flagged at paragraph 131 and 132 of the Explanatory Memorandum her likely intentions for the coverage of the risk management program to 13 different critical infrastructure asset classes.

16. The Department has identified a number of classes of critical infrastructure assets (asset classes) that already have a sufficient or equivalent risk management regime, and the Minister for Home

Affairs has agreed will not be required to comply with risk management program obligations at this time:

- Banking, superannuation, insurance and financial market infrastructure (other than payment systems) assets – covered by Australian Prudential Regulation Authority requirements
- Defence industry assets – covered by the Defence Industry Security Program (other than a small subset of assets connected to the Osborne Naval Shipyard)
- Higher education assets – covered by the UFIT guidelines, and
- Public transport assets – covered by state and territory regulations.

17. In some cases, responsible entities may be subject to existing regulation that only partially addresses the outcomes of this legislation.
18. To avoid a situation where an entity is required to deliver two separate risk management programs, the principles-based rules allow responsible entities flexibility to determine how they deliver a risk management program that would achieve all of the outcomes of the reforms.
19. For example, if you are a responsible entity developing a risk management program you may decide to incorporate existing regulatory compliance measures into your risk management program.
20. Paragraph 272 of the Explanatory Memorandum notes that:

> *State and Territory laws may potentially duplicate components of critical infrastructure risk management programs. This provision [30AN(2)] is intended to ensure the rules can effectively recognise those State and Territory laws to avoid duplicative regulatory burden being placed on industry. For example, the rules may provide that an action done in compliance with a particular State law, which sets security requirements for information technology, would be taken as the required action under this Part.*

## Regulators

21. The Department notes that some submissions queried the role of the Department, the role of the Australian Signals Directorate (ASD) and whether existing regulators for critical infrastructure sectors would be undertaking any responsibilities under the Act.
22. The Department is the default regulator for the provisions under the Act, including for the proposed provisions of the Bill. This includes ensuring education, engagement and compliance with obligations under all provisions of the Act, such as:
    - Part 2—Register of critical infrastructure assets
    - Part 2A—Critical infrastructure risk management program
    - Part 2B—notification of cyber security incidents
    - Part 2C—Enhanced cyber security obligations, and
    - Part 3A—Government assistance.
23. The ASD **does not** have a role as a regulator under the Act or the Bill. The ASD's functions are limited to:
    - Receiving cyber incident reports from responsible entities for critical infrastructure assets under sections 30BC and 30BD of the Act (under Part 2B of the Act), and
    - responding to requests from the secretary for an intervention request under section 35AX of the Act (under Part 3A of the Act).

24. In respect of cyber incident reports under Part 2B of the Act, the Minister may prescribe another Commonwealth Department or statutory agency to receive cyber incident reports (see section 30BF). If the Bill is passed, the Minister will also have capacity to prescribe that another Commonwealth Department or agency is the 'relevant Commonwealth regulator' for the critical infrastructure risk management program obligation (see definition in section 5 of the Act).

25. The Minister is likely to consider prescribing an alternate 'relevant Commonwealth regulatory' in circumstances where an existing Government Department or Agency already has key responsibilities for a critical infrastructure sector. For example, the Minister intends to specify that the Reserve Bank of Australia will act as the regulator for responsible entities of payment systems, for the purposes of their critical infrastructure risk management program obligations.

### Compliance posture

26. The Department has been very clear in all communications and engagements on these reforms that we are committed to supporting businesses to build towards their obligations under the Bill, taking a common sense and business-focused approach to uplift practices and bring them into line with their obligations.

27. The August 2020 discussion paper on the proposed critical infrastructure reforms, reinforced the compliance approach outlined in Critical Infrastructure Centre Compliance Strategy, which stresses voluntary compliance and assistance as the overwhelming regulatory compliance posture.

28. The Department will not actively seek to penalise businesses for failing to comply with new obligations from the date of commencement of the legislation and rules. While there will be circumstances where civil penalties may be sought, first and foremost, the Department's approach will be to educate stakeholders, and create a clear understanding of what is required by the legislation.

29. Detailed guidance on how to meet all requirements under the Bill (and the Act) will be released over the coming weeks. This guidance material is intended to be a living document, where concerns raised by Industry can be addressed to ensure other stakeholders can learn from the same advice.

## Definitions

30. The Department notes that various submissions highlighted concerns with several asset definitions that were introduced in the SLACI Act 2021 that passed into law on 2 December 2021.

### Critical hospital

31. One submission[1] recommended that private hospitals should be excluded from the definition of critical hospitals. The rationale provided is that the legislation does not adequately take into account the complexities and inter-dependencies for operators that run hospitals both with and without intensive care units (ICU) and that the submitter was concerned that it would be placed at a financial disadvantage compared with operators of private hospitals that do not operate ICU departments.

32. The SLACI Act 2021 introduced the definition of critical hospital. This definition was first released for exposure draft in December 2020, and was consulted on prior to being released in the exposure draft. Where an entity operates both hospitals that have an ICU department and those that do not, only those hospitals that have an ICU department will be considered critical hospitals. The Government's policy position reflected in the Bill, and one that has been agreed by Commonwealth and state and territory health stakeholders, is that any hospital with an ICU should be regarded as a

[1] Ramsay Health Care submission to the [Parliamentary Joint Committee on Intelligence and Security] review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, (Submission 19)

critical hospital as these are the hospitals that are integral to the sustainment of life in Australia. It is imperative that these hospitals benefit from an effective and practical uplift to their security and resilience in a time where the threat of all hazards are increasingly present.

## Data storage or processing

33. Some submissions[2] have expressed concerns that the revised definition of "data storage or processing service" may inadvertently capture non-critical entities and recommended further amendments to narrow the scope. Notably, other submissions[3] support the amended definition as it provides industry with much needed clarity about the scope of assets captured.

34. The Department has worked closely with this sector on the asset definition and ensuring that the disparate views across the sector have been considered in finalising the asset definition. In response to feedback on the Bill, the Department has proposed the removal of the requirement for the asset to be providing a commercial service (this now being included in the *data storage or processing service* definition) and to exclude from the definition an asset that is captured by any other class of critical infrastructure asset so that other assets, in particular critical telecommunications assets, are not incidentally captured.

35. Further, if the asset provides data storage or processing services to Commonwealth, State or Territory agencies, the definition now requires the asset to be used to provide a service involving 'business critical data' (such as the personal information of at least 10,000 individuals under the *Privacy Act 1988*, information needed to operate a critical infrastructure asset or relating to risk management and business continuity of a critical infrastructure asset).

36. These amendments serve to restrict the definition to a more accurate capture of the critical assets in this sector.

37. If further restriction of the definition is required, including where representations are made to the Department or the Minister, it is open to the Minister to make a legislative instrument under subsection 9(2) of the Act to exclude additional assets from being a 'critical data storage or processing asset'.

## Telecommunications

38. One submission[4] expressed concern that the 'critical telecommunication asset' definition will almost impact every aspect of public telecommunications infrastructure and services. The Department has already provided further explanations for the amendments to the 'critical telecommunication asset' definition in the Explanatory Memorandum[5], which are intended to align the definition of a 'critical telecommunications asset' with the relevant provisions of the *Telecommunications Act 1997*.

39. Other submissions[6] welcomed the amendments to the 'critical data storage or processing asset' definition as it provides the telecommunications industry with much needed clarity about the scope of critical infrastructure assets, stating this removes the issue of conflicting obligations for assets that fall within both the 'communications' and 'data storage or processing' sectors. The Department

[2] Submission 12, UNSW Allens Hub; Submission 18, Information Technology Industry Council; Submission 41, Communications Alliance; Submission 44, Business Council of Australia
[3] Submission 23, Amazon Web Services
[4] Submission 21, Internet Association of Australia
[5] Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022: Explanatory Memorandum (2022) p16, para 34.
[6] Submission 21, Internet Association of Australia; Submission 37, Telstra

accordingly agrees with these submissions and considers it appropriate to maintain these amendments to provide industry with clarity.

## Critical infrastructure risk management programs

40. The Department notes that submissions highlighted the importance of leveraging international standards and certifications to demonstrate compliance with Australian requirements. The Department has made amendments to the Bill to enable rules to be made which specify existing standards or frameworks, including international standards and certifications, to meet the risk management framework obligations.

41. One submission[7] opined that there should not be an exemption for entities who are 'certified strategic' under the Hosting Certification Framework (HCF) until that framework is legislated or formalised under the Protective Security Policy Framework, though the recognition of the HCF was welcomed by another submission[8]. As communicated by the Department throughout the consultation process, the Bill expressly prohibits unnecessary duplicate existing frameworks where those would achieve the same result. Moreover, the Department sought the inclusion of the HCF at the insistence of a range of stakeholders throughout the consultation process on the rules, which has been highlighted by the submissions to the Committee supporting the inclusion of the HCF.[9]

42. It was suggested that there should be a rule that exhaustively establishes what is required by a risk management program,[10] and further that the Minister should consider input from relevant entities on the requirements stipulated in the rules, despite the Minister having this requirement under proposed paragraph 30ABA(2)(c)[11]. The Department has received feedback that is more appropriate to provide responsible entities with the flexibility to manage their own security in accordance with their business' and sector's needs and the majority of submissions support the position stated in paragraph 237 of the Explanatory Memorandum that "*the critical infrastructure risk management program obligation needs to be flexible and adaptable to the business processes and environment of an individual responsible entity*.." It is also not possible to prescribe 'exhaustive' requirements that are appropriate for every critical infrastructure asset and the context in which that asset operates, given the scale and scope of these reforms. The Department is positioned to support entities as they develop their risk management programs, and will provide detailed guidance on what a business should be considering in developing their risk management programs.

### Timeframes for compliance

43. A number of submissions expressed concern at the proposed timeframes required for compliance with the risk management program rules, with many requesting that the 'grace period' be extended from 6 months to 12 months.[12] One submission recommended that the reporting requirement for the first year of the program should be a readiness attestation, going to an entity's readiness to comply with the requirements of the Act. One submission was concerned that there were no longer grace periods proposed in the rules (noting, however, that the grace period will be given effect via the rules to be made under proposed section 30AB of the Act).

44. Throughout the consultation with industry on the risk management program rules the Department has adjusted the timeframes required for compliance based on feedback from industry, aligning them

[7] Submission 5, Macquarie Telecom Group
[8] Submission 23, Amazon Web Services
[9] Submission 23, Amazon Web Services; Submission 25, Palo Alto Networks; Submission 30, Microsoft
[10] Submission 7, Australian Logistics Council
[11] Submission 13, au Domain Administration
[12] Submission 22, CitiPower, PowerCor and United Energy

with the intent of the legislation to uplift security as well as balancing the considerations of industry, in particular in regards to the cyber and information security rule.

45. Moreover, the Department notes that further consideration can be deferred until formal consultation on the rules occurs, should Parliament pass the Bill. The current proposed grace period remains at 6 months for all but the cyber hazards rule, but the Minister can determine the 'grace' period when making the rule. The Bill's risk management program draft rules have been developed so as to ensure that they are not sufficiently burdensome, that a grace period is to apply, and would note that in consultation with industry many noted that they were already complying with, or exceeding, what would be required under the draft risk management program rules.

## Screening of personnel

46. The Department notes a number of submissions raised concerns about the proposed AusCheck background checking rules in relation to critical workers. These concerns centred on employers using the requirement for background checks to curtail the rights of employee representatives to access certain workplaces, and would require onerous AusCheck background checks that could constitute a threat to privacy and civil liberties.

47. Employee screening, such as requiring criminal history checks, is already common practice across many critical infrastructure sectors. Background checking of people holding critical roles may be a reasonable and proportionate response to the insider threat that Australia's critical infrastructure faces.

*48.* The draft rules do not require any person to undergo a background check through the AusCheck Scheme. The draft rules provide that a responsible entity may apply an AusCheck scheme background check where it may be an appropriate mechanism to manage personnel risks to an asset. This is not the only method an entity can identify to ensure that critical positions or persons in an organisation are held by persons appropriate to do so. Entities responsible for critical infrastructure entities may continue existing practices, such as requiring criminal history, as a means of managing risks consistent with their positive security obligations. The Department will engage with sectors on the nature of the scheme they could choose to use.

49. As specified in paragraph 218 of the Explanatory Memorandum of the Bill, and without prejudicing the consultation process, the use of the AusCheck Scheme for background checking is limited only to a subset of employees, contractors etc. for a responsible entity– not all employees working on or for a critical infrastructure asset. The responsible entity would be required to identify these individuals, and consider whether those employees have access or control over critical aspects of the asset.

50. A 'typical' background check through the AusCheck Scheme is an assessment of information relating to an individual's identity, criminal history, national security assessment, citizenship status, residency status and/or entitlement to work in Australia. Recent amendments to enable criminal intelligence assessments in relation to a background check cannot enable such checks to be conducted under the Act—these are limited to transport security functions under the *Aviation Transport Security Act 2004* and the *Maritime Transport and Offshore Facilities Security Act 2003*.

51. As has been explained in detail and guidance material to stakeholders, the AusCheck scheme **would not** involve the Department accessing or assessing personal internet and email history.

52. If the offences in Schedule 1 to the *AusCheck Regulations 2017* also apply for background checks relating to critical infrastructure, after providing procedural fairness and merits review opportunities to an individual, the outcome of a background check may be that the responsible entity for a critical infrastructure asset is informed that an individual has been convicted of an offence mentioned in item 2.7 of the table in Schedule 1, being "an offence involving, or relating to, participation in, or association with, serious and organised crime or gangs". No further information would be provided

to the entity, protecting the employee's privacy while balancing the need to ensure security. The responsible entity would then detail the mitigations against this risk in their critical infrastructure risk management program, which could involve reassignment to, or offering the individual roles in another area of the business, or ensuring that other risk mitigations are put in place.

53. The Bill does not provide a mechanism to disqualify an applicant from holding a particular position or working on a critical infrastructure asset based on a criminal conviction. Rather, the Department would provide the responsible entity with information regarding the conviction, and it would be the responsibility of the responsible entity to manage that risk.

54. Evidence was also provided about screening processes currently being adopted by employers in purported compliance with the Bill. The Department stresses that the Bill is still subject to the consideration of Parliament and has consistently emphasised to industry that they are under no obligations under the Bill until the Act commences, and in the case of the critical infrastructure risk management program obligations, until those obligations are 'switched on' by the rules under proposed section 30AB. In addition, regulations made under the *AusCheck Act 2007* will be established to define the process for the use of the AusCheck Scheme for critical infrastructure.

55. The Bill does not enable employers to use the using the background check including through the AusCheck Scheme, or any other elements of the critical infrastructure risk management program rules, to dismiss or otherwise disproportionately impact an employee. Responsible entities must manage their obligations under the Act and accompanying rules with existing obligations to their employees, such as under the *Fair Work Act 2009.* The draft personnel security rules detail protections required for critical employees that require persistent, ongoing access to critical systems of critical infrastructure assets, and will not prevent access to a site for legitimate purposes, such as by union representatives performing protected actions.

## Declarations of systems of national significance

### Guidance and consultation on declaration

56. The Department notes that several submissions have recommended that more detailed criteria for the Minister to declare a SoNS should be made publically available[13] and that the decision should be subject to merits review given the impact of such a declaration (noting that the decisions have always been subject to judicial review).[14] One stakeholder suggested that there is no clear guidance on the rights and obligations of critical infrastructure operators that are not themselves designated SoNS but have enterprise end-users that are designated SoNS.[15] Several submissions noted that they considered the consultation period for a SoNS declaration to be too short.[16]

57. The Department will work closely with industry to develop, and iterate as necessary, practical and useful guidance. However, the Department notes that a high legal threshold must be met to be declared a SoNS, which will result in a very small subset of critical infrastructure assets being classed as SoNS.

[13] Submission 10, AGL; Submission 16, Australian Information Industry Association; Submission 18, Information Technology Industry Council; Submission 19, Ramsay Healthcare; Submission 26, Australian Banking Association; Submission 32, Group of Eight; Submission 44, Business Council of Australia
[14] Submission 12, UNSW Allens Hub; Submission 42, Law Council of Australia
[15] Submission 14, BSA Software Alliance
[16] Submission 13, au Domain Administration; Submission 16, Australian Information Industry Association; Submission 21, Internet Association of Australia; Submission 23, Amazon Web Services; Submission 26, Australian Banking Association; Submission 33, Internet Australia, Submission 41, Communications Alliance

58. Stakeholders have proposed adjustments to the consultation requirements, both before and after the Minister considers making a declaration. The current criteria is consistent with the other consultation requirements in the Act, appropriately balancing national security considerations with effective dialogue with entities.

59. Should the Minister seek to declare a SoNS, the Minister must undertake a **28-day consultation period** with the responsible entity of the asset. Should the Minister proceed with the declaration, the responsible entity and any direct interest holders in the critical infrastructure asset must be notified **within 30 days** that the declaration has been made.

# Enhanced cyber security obligations

### Access to system information

60. A number of stakeholders expressed concerns around access to system information. Generally, there were views that the provisions lacked specificity and gave broad discretion on behalf of the Secretary, with several stakeholders noting that the power should be exercised by an independent authority or a judicial officer and should be subject to strict safeguards and oversight mechanisms and should be reviewable[17]. Another stakeholder suggested that there be a right to request, rather than a power to compel the provision of system information.[18]

61. In relation to system information software, it was suggested that a mandatory review process by an independent body of experts to assess the security of the software to be installed, technical feasibility, and the necessity of installing such software[19]. Further, several stakeholders requested clarity around liability in relation to this provision, one noting that entities should be exempt from liability (and indemnified from losses) arising out of disruption or other problems caused by the installed software.[20]

62. Proposed access to system information powers are necessary to protect the very small subset of Australia's most critical infrastructure assets, which all Australians and other critical infrastructure assets rely upon. Paragraphs 458-459 of the Explanatory Memorandum to the Bill explains the meaning of system information and its importance:

> *System information is data generated about a system for the purposes of security, diagnostic monitoring or audit, such as network logs, system telemetry and event logs, alerts, netflow and other aggregate or metadata that provide visibility of malicious activity occurring within the normal functioning of a computer network.*
>
> *System information is crucial to quickly identifying a system or network compromise, tracing that compromise to initial access to mitigate against similar attacks, and understanding the impacts of a compromise and the current state of a system in order to deploy a rapid and effective response to mitigating a cyber incident and restoring functionality.*

63. Further, proposed sections 30DK and 30DD mandates consultation with the entity prior to any system reporting notice being issued. There are no exceptions to this requirement. Furthermore, section 30DJ provides that system information software can only be installed where the Secretary believes on reasonable grounds that the entity is not technically capable of otherwise providing system information itself. This process will ensure the entity has an opportunity to raise any concerns

[17] Submission 13, au Domain Administration; Submission 14, BSA Software Alliance; AIIA, Submission 25, Palo Alto, Submission 30, Microsoft
[18] Submission 14, BSA Software Alliance
[19] Submission 14, BSA Software Alliance
[20] Submission 12, UNSW Allens Hub; Submission 14, BSA Software Alliance; Submission 23, Amazon Web Services; Submission 26, Australian Banking Association; Submission 30, Microsoft; Telstra

about unintended consequences of the provision of system information, whether by the entity itself or through the installation of the software.

64. Receipt of this information will be crucial to the development of a near-real time threat picture which will allow the Government to share actionable, anonymised information back to industry to assist relevant entities improve their cyber resilience. The Government will partner with these responsible entities of designated SoNS to manage risks, including any unintended consequences that may arise, through the implementation phase of these reforms.

### Consultation prior to activation of obligations

65. Several submissions have recommended that detailed decision-making criteria for the Secretary's decisions to apply an ECSO be made publically available, or have made recommendations relating to consultation requirements.[21]

66. As mentioned in the Department's submission in February 2022 to the Committee, the Bill has introduced additional criteria that the Secretary must have regard to before making a decision to activate any of the enhanced cyber security obligations ***prior*** to issuing notices. The criteria are:

- the costs that are likely to the affected entity by complying with the obligations,
- the reasonableness and proportionality of the notice, and
- any other matter the Secretary considers relevant.

67. The Explanatory Memorandum outlines other matters that the Secretary may consider relevant. These include, but are not limited to, international trade obligations that apply, whether the entity is, or has been, subject to other enhanced cyber security obligation, and whether the entity is subject to another regulatory regime under Commonwealth, State or Territory law that is similar.

68. The introduction of these additional criteria were in response to both government and industry feedback. The updated consultation requirements will enable meaningful and effective dialogue with entities, whilst providing administrative safeguards for decisions made to impose cyber security obligations.

## Protected information regime

### Enhanced information sharing

69. Stakeholders continue to express concern that the provisions are not sufficiently specific to enable entities to determine when they may be able to share protected information. Some submitters were generally supportive of increasing transparency so that all parties responsible for protecting critical infrastructure can share best practice.

70. Submitters representing the water sector expressed concerns that the existing authorised disclosure provisions and exemptions were insufficient to permit entities sharing information about their risk management program in the ordinary course of business.[22] And that proposed section 43E over-regulates the use and disclosure of protected information by requiring Secretary consent.[23] These concerns were also echoed by the Communications Alliance in the context of SoNS, recommending that section 43E(3) be removed and section 46(4)(b) be retained so that entities can

[21] Submission 10, AGL; Submission 13, au Domain Administration; Submission 16, Australian Information Industry Association; Submission 23, Amazon Web Services; Submission 25, Palo Alto Networks; Submission 32, Group of Eight; Submission 41, Communications Alliance;
[22] Submission 24, Water Services Association of Australia; Submission 45, Sunwater Ltd.
[23] Submission 45, Sunwater Ltd.

decide when it is appropriate to disclose protected information to relevant entities within their supply chain when reasonable necessary.[24]

71. The Department has ensured the protected information regime has been designed with two key purposes in mind. The first is to ensure that any information of a sensitive nature is prevented from unauthorised disclosure, whether that information is commercially sensitive, personal information or where disclosure of that information may jeopardise the defence, national security or stability of Australia, the Australian people or the Australian economy. The second purpose is to balance those considerations with the transfer of that information where it is appropriate or beneficial, such as where the sharing of that information will allow the development of appropriate risk mitigations.

72. In general terms, the lawfulness of disclosure of protected information under the Act turns on who the disclosure is to, and the purpose of the disclosure to that person. Responsible entities will need to consider the lawfulness of a proposed disclosure to a stakeholder on a case by case basis with a clear understanding of the **purpose of the disclosure**. For clarity, the Bill provides for sharing of information where an entity is disclosing that information to ensure compliance with the Act, or where that entity is disclosing the information in good faith compliance with obligations under the Act.

## Disclosure to oversight bodies

73. The Office of the Inspector-General of Intelligence and Security (IGIS) submitted its concern that entities may be prevented from voluntarily disclosing protected information to her office for an authorised purpose under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act).[25] The Office of the Australian Information Commissioner (OAIC) raised concern that as there is no express authorisation or exemption in the Act to permit disclosure of protected information to the OAIC, the Act would prevent entities from submitting reports of notifiable data breaches that relate to protected information under the *Privacy Act 1988*. The OAIC and the Commonwealth Ombudsman further expressed concern that section 47 of the Act would allow entities to refuse to provide information requested by the OAIC.[26]

74. Section 46(1) of the Act includes an exception to the offence for unauthorised use or disclosure of protected information if the disclosure is required or authorised by a law of the Commonwealth. In other words, where another Commonwealth law requires or authorises the use or disclosure of protected information and information is used or disclosed in accordance with that provision, the use or disclosure of any protected information will not amount to an offence under the Act. Where information is provided to IGIS, and where that information is provided for a purpose listed in section 34B(1) of the IGIS Act, section 46 would apply so that such use or disclosure does not amount to an offence for the purposes of the Act. Similarly, section 46 would not prevent the reporting of notifiable data breaches, as they are required to be reported under Part IIIC of the *Privacy Act 1988*.

75. Section 47(1) of the Act (as amended by the SLACI Act 2021) provides that:

> *An entity is not (subject to subsection (2)) to be required to disclose protected information, or produce a document containing protected information, to … a tribunal, authority or person that has the power to require the answering of questions or the production of documents.*

[24] Submission 41, Communications Alliance
[25] Submission 35, Office of the Inspector-General of Intelligence and Security.
[26] Submission 11, Commonwealth Ombudsman; Submission 31, Office of the Australian Information Commissioner

76. Section 47(2) of the Act was inserted by the SLACI Act 2021, recognising the important oversight role that the IGIS has in relation to the operations of the ASD. This provision relevantly states that:

> *Subsection (1) does not prevent an entity from being required to disclose protected information, or to produce a document containing protected information, if it is necessary to do so for the purposes of giving effect to … the Inspector-General of Intelligence and Security Act 1986, or any other Act that confers functions, powers or duties on the Inspector-General of Intelligence and Security*.

77. Additionally, sections 43A-43C of the Act provide authorised use and disclosure of protected information to both the IGIS and the Commonwealth Ombudsman for the purpose of officials from those agencies exercising powers or performing functions and duties under each of their respective legislation. These provisions enable the entities involved in oversight of the Act to have the information required to perform their functions.

78. As described above, where an entity is required or authorised by a law of the Commonwealth to provide information to the OAIC or the Commonwealth Ombudsman (for example, under the *Privacy Act 1988*), section 46(1) ensures that the Act does not prevent this. However, due to the sensitivity of protected information, the intention of the Act remains to ensure that there is discretion to resist disclosure of this information in court proceedings that are not related to the operation of this Act or the IGIS Act or the IGIS' functions, powers or duties under any other Act.

## Immunities and other protections

79. A number of submitters raised a concerns that the immunities provisions, while expanded to include a broader range of entities, still had a number of gaps, including:

- while extended to contract services providers to the regulated entity, contracted service providers to related companies are not sufficiently protected
- while the immunities apply with respect to specific obligations, but do not apply generally for the purpose of actions done to implement or improve processes to ensure that the entity has the capability to comply with the Act in the future
- do not apply to acts done in preparation for future regulatory obligations and
- only protected for actions for damages, and not other causes of Action.[27]

80. The immunity provisions have been specifically drafted to protect an entity where it complies with specific actions under the Act. Immunity provisions have been sufficiently expanded to capture entities that may be subject to risk of action for damages in compliance with the SOCI Act. The Government has consciously decided to not expand the immunity provisions for preparatory actions, particularly where those preparatory actions are not done in accordance with the Act as it is in force from time to time.

## Conclusion

80. The Department trusts that this supplementary submission, read alongside the Department's previous submissions and evidence provided before the Committee, will assist in providing an understanding of the Bill's proposed operation.

81. The Bill relies on Government and industry partnerships to succeed. If passed, the reforms will deliver an effective and practical uplift to the security and resilience of Australia's critical

[27] Submission 23, Amazon Web Services, Submission 37, Telstra; Submission 42, Law Council of Australia; Submission 44, Australian Banking Association.

infrastructure, as well as providing for a regime for greater protections for those critical infrastructure assets that are crucial to Australia, and would lead to cascading consequences of disruption to other critical infrastructure assets and sectors if they are unavailable.

82. The Department thanks the Committee for its consideration of the Bill, and industry for its robust and proactive engagement to date.