29 February 2024

BSA COMMENTS ON CYBER SECURITY LEGISLATIVE REFORMS CONSULTATION PAPER

Submitted Electronically to the Department of Home Affairs

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the Department of Home Affairs (**DHA**) on the Cyber Security Legislative Reforms Consultation Paper (**Consultation Paper**),[2] issued to implement the 2023-2030 Australian Cyber Security Strategy (**Strategy**).[3]

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Our members have made significant investments in Australia, and we are proud that many Australian companies and organisations continue to rely on our members' products and services to do business and support Australia's economy.

We welcome the Australian Government's efforts to implement the Strategy. BSA recognises that increased connectivity, computing, and data storage needs require creative solutions to maintain effective cybersecurity. We support Australia's efforts to ensure that its cyber security laws remain fit-for-purpose and capable of addressing ever-evolving cyber threats. Cyber security is a shared responsibility across public and private stakeholders, and effective legislative reform requires close coordination between industry and government in both formulation and implementation. In this regard, we are heartened that Australia is committed to co-designing these reforms with industry partners.[4]

Summary of BSA's Recommendations

Part 1: New cyber security legislation

Measure 1: Secure-by-design standards for Internet of Things (**IoT**) devices

1. Align with internationally recognised standards when developing a mandatory cyber security standard for consumer-grade IoT devices, and take every effort to avoid a divergence of approach with other countries. In this regard, while BSA supports the adoption of the ETSI EN 303 645 standard, we urge recognition and acceptance of other similar internationally recognised standards, such as the ISO/IEC 27402.

---

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper, December 2023, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2023-30-consultation-paper.pdf.

[3] 2023-2030 Australian Cyber Security Strategy, November 2023, https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf. 2023-2030 Australian Cyber Security Action Plan, November 2023, https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy-action-plan.pdf.

[4] Consultation Paper (2023), p. 4.

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

Measure 2: Ransomware reporting for businesses

2. Reporting should only be mandatory if an entity makes a ransomware or extortion payment. If an entity is only targeted by an attack or receives a demand, reporting should be optional, and more details are required on when such a report should be made.

3. Do not impose additional ransomware reporting obligations on entities which are already subject to existing incident reporting obligations, such as those set out in the *Security of Critical Infrastructure Act 2018* (**SOCI Act**).

4. Lower the annual turnover threshold for reporting entities. In this regard, consider setting the threshold at A$3 million, which is aligned with the definition of "small business" in the *Privacy Act 1988* (**Privacy Act**).

5. Incorporate "no-fault" and "no-liability" principles into the ransomware reporting obligation.

Measure 3: Limited use obligation for information provided to the Australian Signals Directorate and the National Cyber Security Coordinator

6. Define the types of information that would be shared, specify all purposes that the shared information will be used for, and clearly state that the shared information shall not be used for any purpose other than those specified in legislation.

7. Introduce requirements to seek the affected entity's consent before sharing information with other agencies, and ensure that there are adequate safeguards protecting such information from unauthorised access or disclosure, and that the information will not be used in any regulatory action against the reporting organisation

Measure 4: Establishing a Cyber Incident Review Board (**CIRB**)

8. Require the CIRB to obtain express consent from affected entities to disclose potentially confidential information, including the names of said affected entities, ahead of releasing the report.

9. Prioritise appointing industry experts to be part of the CIRB, and provide a transparent process for application.

10. Clearly state that information obtained from conducting a review cannot be used for any investigation or compliance activities.

11. Do not vest the CIRB with powers to require entities to provide information.

12. The threshold for when a CIRB review can be initiated should be set at when a cyber incident of "significant impact" has occurred, per the SOCI Act. The review should be initiated by the CIRB itself, with majority agreement.

Part 2: Amendments to the Security of Critical Infrastructure Act 2018

Measure 5: Data storage systems and business critical data

13. Critical infrastructure entities should consider data storage systems as part of their critical infrastructure assets and manage the risks accordingly. Amendments should continue ensuring that critical infrastructure entities are responsible for interfacing directly with regulators and avoid imposing direct obligations on the entities' service providers.

Measure 6: Consequence management powers

14. Refrain from introducing a new consequence management power, as the existing power in section 32 of the SOCI Act is sufficient for post-incident consequence management.

15. The scope of the proposed consequence management power is too broad, and should be substantially reduced if implemented. Further, there must be clear and precise safeguards guiding its exercise. Terms such as "unwilling", "causal link", "relevant impact" and "imminent" are vague and subjective, and as such are ineffective checks on this proposed power.

16. Introduce independent oversight mechanisms and allow for limited judicial review to check the exercise of the proposed consequence management power and other similarly broad powers vested in the Government under the SOCI Act.

Measure 7: Simplifying protected information provisions

17. Change the term "Protected Information" in the SOCI Act to "Restricted Information" to avoid further confusion between the "Protected Information" in the SOCI Act and the "Protected" security classification in the Protective Security Policy Framework.

18. Introduce requirements to seek the affected entity's consent before sharing protected information with other government entities, and ensure that there are adequate safeguards protecting such information from unauthorised access or disclosure.

Measure 8: Review and Remedy Powers

19. Refrain from introducing a new review and remedy power, given that the CIRMP-related obligations are not yet fully operational and there is no clear evidence that the Government requires such a power.

20. If introduced, define key terms (notably, "seriously deficient" and "material risk") to properly scope the exercise of the power, subject the power to independent oversight, and provide affected entities with the right to appeal/review the Government's exercise of the power. .

Measure 9: Telecommunications sector security under the SOCI Act

21. Consolidate security regulation for the telecommunications under the SOCI Act, and continue identifying opportunities to streamline and simplify complex cyber security requirements.

Part 1: New cyber security legislation

Part 1 of the Consultation Paper contemplates legislative measures that aim to address various gaps in Australia's current cybersecurity legislative framework. Generally, the proposed measures signify the Government's commitment to build a resilient cyber ecosystem that emphasises cooperation across public and private sectors, aiming for a unified approach to cybersecurity as opposed to perpetuating a culture of ascribing blame when incidents occur. This policy intent is reflected in the proposed measures, most notably the "no-liability" protection principles, the limited-use obligation, and the establishment of the CIRB with industry stakeholders.

BSA is supportive of this general approach to cybersecurity – cybersecurity is a team sport, and ever-evolving cyber threats must be countered by a united front.

Measure 1: Secure-by-design standards for Internet of Things devices

Measure 1 proposes to establish a mandatory standard for consumer-grade IoT devices. In establishing this standard, the Government seeks to "align with international standards, ensure consistency between jurisdictions and minimise regulatory burden on Australian businesses, while also meeting [Australia's] national security objectives".[5]

Most effective laws and policies in the cybersecurity space leverage internationally recognised standards and best practices. Governments can reduce redundancy by leveraging internationally recognised standards for cybersecurity certifications and accepting certifications from liked-minded allies. To that end, BSA supports the adoption of the ETSI EN 303 645 standard, which is used by many of Australia's partners, such as the EU, India, Japan, Singapore, and the United Kingdom. This is also in line with the Quad Principles on Critical and Emerging Technology Standards (**Quad Principles**),[6] where the Quad members affirmed their support for "private sector-led, consensus-based, and multi-stakeholder approaches to international standards development that foster

[5] Consultation Paper (2023), p. 9.

[6] Quad Principles on Critical and Emerging Technology Standards, May 2023, https://www.pmc.gov.au/sites/default/files/resource/download/quad-principles-critical-emerging-technology-standards.pdf.

interoperability, compatibility, and inclusiveness." Specifically, the Quad Principles stated that technology standards "should promote interoperability, innovation, trust, transparency, diverse markets, security-by-design, compatibility, inclusiveness and free and fair market competition" and that the members "[s]upport technology standards that promote interoperability, competition, inclusiveness and innovation."

Proposing a mandatory standard in Australia goes beyond the approach of other countries that are considering or have adopted a voluntary labelling scheme. We strongly advise that every effort be taken to avoid a significant divergence of approach across countries. Relatedly, even if ETSI 303 645 is the basis for developing Australia's mandatory cyber security standard for consumer-grade IoT devices, this does not preclude Australia from recognising and accepting other similar internationally recognised standards. In the spirit of interoperability and compatibility, as well as minimising regulatory burden, BSA recommends that Australia recognise and accept other internationally recognised standards, such as the ISO/IEC 27402:2023 standard (ISO/IEC 27402). ISO/IEC 27402 specifically sets out a globally harmonised approach to baseline security and privacy requirements of IoT devices, and it drew from many existing standards and best practices, such as the C2 Consensus on IoT Security Baseline Capabilities and an interagency report from the US National Institute of Standards and Technology (**NIST IR 8259A**), as well as ETSI EN 303 645 itself. As such, businesses that meet the standards in ISO/IEC 27402 should also be deemed to meet the baseline contemplated in Australia's proposed standard for IoT devices. Australia should also continue to work closely with industry on the implementation.

Recommendation 1: Align with internationally recognised standards when developing a mandatory cyber security standard for consumer-grade IoT devices and take every effort to avoid a divergence of approach with other countries. In this regard, while BSA supports the adoption of the ETSI EN 303 645 standard, we urge recognition and acceptance of other similar internationally recognised standards, such as the ISO/IEC 27402.

Measure 2: Ransomware reporting for businesses

Measure 2 proposes to establish a ransomware reporting obligation for two situations: a) if an entity is impacted by a ransomware or cyber extortion attack and receives a demand to make a payment to decrypt its data from being sold or released; and b) if an entity makes a ransomware or extortion payment.[7]

BSA recommends that the mandatory reporting obligation should only apply in Situation (b) i.e., if an entity makes a ransomware or extortion payment. We acknowledge that limited visibility of ransomware attacks restricts the capability to respond to these attacks, and that enhanced reporting obligations will provide a better threat picture that will bolster our collective security. However, with regard to Situation (a), which mandates a ransomware report whenever an entity is "impacted" by an attack and receives a "demand", it is not clear what exactly the threshold is for businesses to report such incidents. For example, an entity may receive an extortion email threatening to release sensitive information unless a payment is made, but it is not clear if this constitutes being "impacted" or receiving a "demand" for the purposes of reporting. This creates uncertainty for businesses while also adding to their regulatory burden. Furthermore, as a general principle, reporting requirements should focus on the most significant incidents, thus avoiding the noise that can come from an overly broad approach. If Situation (a) is retained, we suggest that the reporting obligation be made voluntary, and recommend that more details be provided on when an entity should make the report.

Recommendation 2: Reporting should only be mandatory if an entity makes a ransomware or extortion payment. If an entity is only targeted by an attack or receives a demand, reporting should be optional, and more details are required on when such a report should be made.

On which entities are required to report, the Consultation Paper observes that an entity may already be subject to other incident reporting obligations, citing the reporting obligations in the SOCI Act as an

[7] Consultation Paper (2023), p. 14.

example. As such, the Consultation Paper suggests that "it may be appropriate to acquit the proposed ransomware reporting obligation through existing reporting obligations".[8] BSA agrees with this suggestion and strongly recommends that any ransomware reporting obligations should only apply to entities which are not already subject to existing incident reporting obligations. There has been a proliferation of cyber security laws, policies, and initiatives in recent years, which created a regulatory landscape that is difficult for businesses to navigate. For example, while there is currently no universal requirement for Australian businesses to report cybersecurity incidents, there are several mandatory reporting obligations for specific types of businesses that are spread across multiple pieces of legislation.[9] These overlaps have added unnecessary complexity in the overall cybersecurity regime, making it difficult for businesses of all sizes to understand and meet their compliance obligations. Streamlining and simplifying Australia's reporting obligations will improve understanding and compliance with the regime and will boost overall confidence in Australia's business operating environment.

Recommendation 3: Do not impose additional ransomware reporting obligations on entities which are already subject to existing incident reporting obligations, such as those set out in the SOCI Act.

The Consultation Paper also suggests limiting the scope of the ransomware reporting obligation to specific types of entities, such as businesses with an annual turnover of more than A$10 million a year. This would also exempt small businesses from the new reporting obligation.[10]

BSA recommends lowering the annual turnover threshold for reporting entities. Ransomware attacks are more commonly experienced and have a more damaging impact on small and medium enterprises. While we note that this threshold is aligned with the small business threshold used by the Australian Tax Office, the Consultation Paper itself acknowledges that this "would significantly restrict the sample size for ransomware information".[11] We suggest setting the threshold to an annual turnover of A$3 million, which aligns with the definition of "small business" in the Privacy Act.[12]

Recommendation 4: Lower the annual turnover threshold for reporting entities. In this regard, consider setting the threshold at A$3 million, which is aligned with the definition of "small business" in the Privacy Act.

We are also encouraged by the Government's consideration of "no-fault" and "no-liability" principles to assure businesses that the agency receiving ransomware reports will not seek to ascribe blame to the affected entity for the incident, nor will the affected entity be prosecuted for making a payment. This approach addresses a critical barrier to effective cybersecurity defence: the fear of reputational damage and legal repercussions. By removing the stigma associated with reporting ransomware

[8] Consultation Paper (2023), p. 15.

[9] Examples of prevailing reporting requirements include:

a) Under the Security of Critical Infrastructure Act 2018, and subsequent amendments, critical infrastructure asset owners and operators must report critical incidents (with a "significant impact" on their asset) within 12 hours of becoming aware of the incident, and other security incidents (with a "relevant impact" on their asset) within 72 hours.

b) The Privacy Amendment (Notifiable Data Breaches) Act 2017 amended the Privacy Act 1988 to require organisations to "notify affected individuals and the [Office of the Australian Information Commissioner] when a data breach is likely to result in serious harm to an individual whose personal information is involved". The scheme applies to all organisations covered by the Privacy Act, which includes Australian Government agencies and businesses with annual turnover of more than $3 million AUD. The Attorney General's Office is currently undertaking a substantial review of the Privacy Act.

c) In the financial services sector, the Prudential Standard CPS 234 on Information Security requires entities regulated by the Australian Prudential Regulation Authority (**APRA**) — including banks, insurers, and superannuation funds — to notify the regulator of material information security incidents within 72 hours. Entities must also notify APRA of material information security control weaknesses within 10 business days.

[10] Consultation Paper (2023), p. 15.

[11] Consultation Paper (2023), p. 15.

[12] Privacy Act 1988, Section 6D (Small business and small business operators).

attacks, businesses are more likely to come forward and share crucial threat information, enabling a more rapid and coordinated response to ransomware incidents and ultimately bolstering cyber resilience.

Recommendation 5: Incorporate "no-fault" and "no-liability" principles into the ransomware reporting obligation.

Measure 3: Limited use obligation for information provided to the Australian Signals Directorate and the National Cyber Security Coordinator

Measure 3 proposes to establish a limited use obligation for the Australian Signals Directorate (**ASD**) and the National Cyber Security Coordinator (**Cyber Coordinator**), such that information shared with them would be "limited to prescribed cyber security purposes defined in appropriate legislation".[13]

BSA appreciates that this proposed measure seeks to encourage industry to voluntarily provide information to ASD and the Cyber Coordinator for incident response/management and threat prevention. To ensure that this proposed measure reflects the policy intention, we recommend that the legislation define the types of information that would be shared,[14] specify all the purposes that such information will be used for,[15] and clearly state that the information shared shall not be used for any purpose other than those that are specified, including any possibility of the information being used in any regulatory action against the reporting organisation, not just by ASD and Cyber Coordinator, but any Government agency. This will enhance the certainty of how the limited use obligation will apply, and provides further reassurance to affected entities that regulators cannot liberally interpret the limited use obligation to leverage the information provided to ASD or the Cyber Coordinator as part of an investigation or for compliance activities against them.

Recommendation 6: Define the types of information which will be shared, specify all purposes that the shared information will be used for, and clearly state that the shared information shall not be used for any purpose other than those specified in legislation.

The Consultation Paper notes that the limited use obligation "does not preclude ASD and the Cyber Coordinator from sharing appropriate information with other agencies – including law enforcement national security, intelligence agencies and regulators".[16]

Most, if not all, of the information shared by the affected entity with ASD and the Cyber Coordinator will be sensitive in nature. As such, the legislation should impose safeguards to protect such information, including how and when such information is to be shared with other agencies. At the minimum, ASD and the Cyber Coordinator should seek the affected entity's consent to share the information, and in the process explain to the affected entity *why* the information has to be shared, and with *which* specific agencies. To the extent that such information is to be shared with other agencies, ASD and the Cyber Coordinator should adopt processes to protect such information, including by ensuring that only relevant information is shared. More broadly, given the sensitivity of the information, any agency entrusted with such sensitive information must have strong cyber security

---

[13] Consultation Paper (2023), p. 20.

[14] The Government can refer to the US's *Cybersecurity Information Sharing Act 2015*, which sets out **"cyber threat indicators"**, which are defined as "information that is necessary to describe or identify: (i) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (ii) a method of defeating a security control or exploitation of a security vulnerability; (iii) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (iv) a method of causing a user with legitimate access to an information system or information that is stored on, processed by or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (v) a malicious cyber command or control; (vi) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (vii) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (viii) any combination of (i)-(vii)."

[15] For reference, the US's *Cybersecurity Information Sharing Act 2015* defines a **"cybersecurity purpose"** as "the purpose of protecting an information system or information that is stored on, processed by or transmitting an information system from a cybersecurity threat or security vulnerability".

[16] Consultation Paper (2023), p. 21.

practices in place to protect such information from unauthorised access or disclosure. As mentioned in the previous recommendation, any such information should also not be used by the other agencies in regulatory actions against the reporting organisation.

<u>Recommendation 7</u>: Introduce requirements to seek the affected entity's consent before sharing information with other agencies, and ensure that there are adequate safeguards protecting such information from unauthorised access or disclosure, and that the information will not used in regulatory actions against the reporting organisation.

Measure 4: Establishing a Cyber Incident Review Board

Measure 4 proposes to establish a CIRB to conduct no-fault, post-incident reviews of cyber incidents. The findings and learnings will be shared publicly to enhance collective cyber security and help prevent similar incidents from occurring in the future.

BSA welcomes this proposed measure, as it deepens public-private partnership and engagement in a tangible manner. The public sharing of findings and lessons is particularly valuable, as it enables a wider range of stakeholders to benefit from the insights gained from the CIRB's reviews, thereby strengthening the cyber security ecosystem as a whole. However, there should also be measures in place to prevent confidential information, such as the name of the affected entity and privileged internal communications, from being shared without their consent. As such, while we agree with the stated purpose of such reviews (e.g., to understand details behind the cyber security incident, including the nature of vulnerabilities, how these vulnerabilities are exploited, the remedial actions taken by both industry and government, the impacts of the incident on the affected entity, etc) and how they would be shared with the public (i.e., in the form of a public report that outlines lessons learned, with appropriate recommendations),[17] we recommend that the CIRB be required to obtain express consent from affected entities to disclose potentially confidential information, including the names of said affected entities, ahead of releasing the report.

<u>Recommendation 8</u>: Require the CIRB to obtain express consent from affected entities to disclose potentially confidential information, including the names of said affected entities, ahead of releasing the report.

To ensure that the CIRB can effectively carry out its functions, industry involvement is especially critical. BSA members operate in multiple markets and invest enormous resources in their own cyber security capabilities, and in many cases offer cutting-edge cyber security tools and services, to deal with the latest cyber threats. This allows them to provide insights from a global perspective. They are also well-equipped to give expert opinions on a range of cyber security issues, such as threat detection, risk management, incident response and business continuity planning, as they have experience managing such issues themselves. As such, regardless of how the CIRB is structured, the CIRB should prioritise appointing industry experts as part of its membership and provide a transparent process for application.

<u>Recommendation 9</u>: Prioritise appointing industry experts to be part of the CIRB and provide a transparent process for application.

The no-fault principle is described as "critical" for maximising stakeholder engagement with the CIRB – the Consultation Paper states that the CIRB will not make findings of fault, nor can the outputs and recommendations of a CIRB review be used to make findings of fault.[18] However, it is not clear if the information obtained from the course of the CIRB review process may be used for investigation or compliance activities by any Government agency. Given that the CIRB membership will include representatives from various government agencies, it is important to ensure that the information obtained from the course of conducting a CIRB review cannot be used for any investigation or compliance activities.

[17] Consultation Paper (2023), p. 23.

[18] Consultation Paper (2023), p. 24.

<u>Recommendation 10</u>: Clearly state that information obtained from conducting a CIRB review cannot be used for any investigation or compliance activities.

The proposed measure contemplates providing CIRB with investigatory powers, with two main options: a) voluntary powers to request information but no powers to compel entities to participate in reviews; or b) limited information gathering powers to require entities to provide appropriate information to facilitate the review of cyber incidents. BSA cautions against giving the CIRB the powers contemplated in (b). The CIRB might be tasked to review an incident involving a company that is a competitor of a CIRB representative, and the ability to require the competitor to disclose sensitive information – to the competitor's potential detriment – will undermine the CIRB's objectivity and impartiality.

<u>Recommendation 11</u>: Do not vest the CIRB with powers to require entities to provide information.

On when a CIRB review is to be initiated, we agree that the CIRB should "focus on reviewing significant incidents rather than all cyber incidents". In this regard, we recommend that the threshold for initiating a review could be pegged to the SOCI Act, specifically when a cyber incident has had a "significant impact" on the availability of a critical infrastructure asset.[19] Such incidents will have significant consequences that would warrant a CIRB review. Further, in line with the function and independent nature of the CIRB, the review should only be initiated by the CIRB itself, with majority agreement, and *not* at the discretion of Government representatives (i.e., the Minister for Cyber Security, the National Cyber Security Coordinator, or via agreement between the Minister for Cyber Security and relevant Ministers).

<u>Recommendation 12</u>: The threshold for when a CIRB review can be initiated should be set at when a cyber incident of "significant impact" has occurred, per the SOCI Act. The review should be initiated by the CIRB itself, with majority agreement.

Part 2: Amendments to the Security of Critical Infrastructure Act 2018

Part 2 of the Consultation Paper focuses on potential amendments to the SOCI Act. The proposed amendments seek to "address gaps [in the SOCI Act] identified following recent major cyber security incidents".[20] BSA agrees with the policy intent – it is crucial that the SOCI Act remains fit-for-purpose.

However, a substantial part of these proposed measures involves vesting the Government with more powers to plug said gaps. This raises concerns regarding the necessity, scope, application, and avenues of appeal when such powers are exercised. Australia is a global thought leader on cyber security policy, and its approach is studied closely by other countries in the region. Australia's approach of vesting itself with broad powers may influence other governments to do the same, but rarely do such governments exercise such powers with restraint.

Generally, we urge the Government to refrain from vesting itself with further powers as a solution to address perceived policy gaps, and to the extent that the powers are necessary, their exercise should be subject to independent oversight and rigorous checks.

Measure 5: Data storage systems and business critical data

Measure 5 proposes to: a) include data storage systems holding "business critical data" in the definition of "asset" under section 5 of the SOCI Act; and b) amend the *Security of Critical Infrastructure (Critical Infrastructure risk management program) Rules* (**CIRMP Rules**) to include risks to data storage systems holding "business critical data" and the systems that access the data as "material risks". The Consultation Paper noted that the SOCI Act "does not explicitly require critical infrastructure entities to protect data storage systems that hold business critical data, even if

[19] SOCI Act, Section 30BEA (Significant impact).

[20] Consultation Paper (2023), p. 30.

vulnerabilities in these systems could cause significant disruption or damage to critical infrastructure", and Measure 5 seeks to plug this gap.[21]

BSA supports these proposed changes. We agree that critical infrastructure entities should consider data storage systems as part of their critical infrastructure assets and manage the risks accordingly. We also note that, under the current SOCI Act, the critical infrastructure entities are the parties responsible for interfacing with regulators in a cyber security incident (e.g., making an incident report), even as they use other service providers, including third-party data storage or processing providers, as part of their operations. The proposed amendments should continue to maintain this arrangement, as it clearly allocates roles and responsibilities to different actors along the cyber security "chain".

BSA cautions against any approach or policy that imposes direct obligations on service providers which are further down this "chain" supporting a critical infrastructure entity, as it would create unnecessary regulatory complexity and duplication without enhancing cybersecurity (and in fact, potentially jeopardises cybersecurity as this regulatory complexity obfuscates roles and responsibilities, leading service providers to divert scarce cyber resources from addressing real cyber threats to managing regulatory bureaucracy).

Recommendation 13: Critical infrastructure entities should consider data storage systems as part of their critical infrastructure assets and manage the risks accordingly. Amendments should continue ensuring that critical infrastructure entities are responsible for interfacing directly with regulators and avoid imposing direct obligations on the entities' service providers.

Measure 6: Consequence management powers

Measure 6 proposes to legislate an "all-hazards power of last resort", which will allow the Government to direct an entity to take specific actions to manage the consequences of a national significant incident.[22] This power may only be authorised by the Minister for Home Affairs (**Minister**) if there is no existing power available to support a fast and effective response.

At the outset, it is not clear why such consequence management powers are necessary, given that the SOCI Act already vests the Minister with similar powers. Notably, section 32 of the SOCI Act[23] allows the Minister to issue written directions requiring "a reporting entity for, or an operator of, a critical infrastructure asset to do, or refrain from doing, an act or thing, if the Minister is satisfied that there is a risk of an act or omission that would be prejudicial to security." The Consultation Paper notes that "the Government does not have powers to support industry with post-incident consequence management",[24] but the Minister's existing power appear broad enough that the Minister could issue directions for post-incident consequence management. We therefore urge the Government to refrain from introducing an additional consequence management power.

Recommendation 14: Refrain from introducing a new consequence management power, as the existing power in section 32 of the SOCI Act is sufficient for post-incident consequence management.

The broad scope and applicability of the proposed consequence management power is also cause for concern. This proposed power can be used to, among other things "[d]irect a critical infrastructure entity to do or prohibit from doing a certain thing to prevent or mitigate the consequences of an incident".[25] The scope is therefore extremely broad, much like the existing power in section 32 of the SOCI Act. While the Consultation Paper puts forth various safeguards to guide the exercise of this

[21] Consultation Paper (2023), p. 36.

[22] Consultation Paper (2023), p. 43.

[23] SOCI Act, Section 32 (Direction if risk of act or omission that would be prejudicial to security".

[24] Consultation Paper (2023), p. 41

[25] Consultation Paper (2023), p. 44.

broad power, some of the listed safeguards are vague and present low thresholds that will not act as effective checks. For example:[26]

- The Minister must be satisfied that the critical infrastructure entity is "unwilling or unable" to address the consequences of the incident. However, it is foreseeable that the Government and the critical infrastructure entity may disagree on the best course of action in response to a cyber security incident. In such situations, the Minister can interpret the entity's disagreement as unwillingness to address the consequences, even if the entity has legitimate reasons for taking such a position.
- A direction issued under this power may only be addressed to a critical infrastructure entity. However, there is nothing stating that the critical infrastructure entity needs to be directly impacted by a cyber security incident – instead, all is required is that there must be a "causal link" to an incident impacting a critical infrastructure asset, and that there is a "relevant impact, whether direct or indirect" on the critical infrastructure. Essentially, the power may be used on any critical infrastructure entities that are not directly impacted by a cyber security incident.
- The power can be exercised when the consequence of an event "is imminent". Assessing whether events or its effects are "imminent" is extremely subjective and will cause confusion as to when the power can be exercised.

Recommendation 15: The scope of the proposed consequence management power is too broad, and should be substantially reduced if implemented. Further, there must be clear and precise safeguards guiding its exercise. Terms such as "unwilling", "causal link", "relevant impact" and "imminent" are vague and subjective, and as such are ineffective checks on this proposed power.

In addition, there appears to be no independent oversight mechanisms specified in the Consultation Paper over the exercise of the proposed power. As mentioned above, many of the safeguards are vague and subjective, and do not serve as effective checks. Furthermore, while there are some oversight mechanisms contemplated in the Consultation Paper, these oversight mechanisms only require the Minister to consult within the Government and the affected entity.[27] This is further compounded by the fact that all administrative decisions made under Part 3A of the SOCI Act, which this proposed power will fall under, are excluded from judicial review following amendments to the *Administrative Decisions (Judicial Review) Act 1977* (**ADJR Act**).

Policies that introduce intrusive powers, even for the purposes of upholding cybersecurity, can compromise user confidence in the integrity and trustworthiness of a service provider's products and services, and should therefore be subject to appropriate checks and balances, such as independent authorisation and reviews on the exercise of such intrusive powers.

We recommend implementing additional independent oversight mechanisms to prevent the misuse of such discretion, and to allow for legislative appeal or review of exercise of the power. One possible check is the implementation of a mandatory review process whenever such a power is exercised, during which a panel of independent technical experts assess the security, feasibility, and reasonableness of exercising the power.

In addition, while we recognise that issues relating to security can be urgent and highly sensitive, the Government should consider amending ADJR Act to allow limited judicial review of this proposed consequence management power, as well as other broad powers in the SOCI Act. For example, such rights to judicial review can be deferred, or limited to issues related to the technical feasibility of the Minister's direction and the process of exercising the power. This is preferable to a wholesale exclusion of the right to judicial review.

[26] Consultation Paper (2023), p. 44.

[27] Consultation Paper (2023), p. 44-45.

<u>Recommendation 16</u>: Introduce independent oversight mechanisms and allow for limited judicial review to check the exercise of the proposed consequence management power and other similarly broad powers vested in the Government under the SOCI Act.

Measure 7: Simplifying protected information provisions

Measure 7 proposes to amend the protected information framework in the SOCI Act to simplify how government and industry share information in crisis situations. This involves: a) making clear that entities should take a "harms-based approach" when considering whether to disclose information; and b) allowing entities to disclose information for the purpose of the continued operation of, or mitigation of risks to, a critical infrastructure asset.[28]

As part of the simplification process, we recommend changing the term "Protected Information" to "Restricted Information". This is because the Government's Protective Security Policy Framework (**PSPF**) also uses the word "Protected" in its security classification, and this has led to substantial confusion between the "Protected Information" in the SOCI Act and the "Protected" security classification in the PSPF. In fact, the Cyber and Infrastructure Security Centre thought it necessary to explain this distinction on its website,[29] highlighting the potential for confusion.

<u>Recommendation 17</u>: Change the term "Protected Information" in the SOCI Act to "Restricted Information" to avoid further confusion between the "Protected Information" in the SOCI Act and the "Protected" security classification in the PSPF.

The Consultation Paper suggests that "provisions relating to government entities should be broadened to allow disclosure of protected information to all Commonwealth, state and territory government entities regardless of policy responsibility, where disclosure is necessary for the purpose of upholding the security and resilience of critical infrastructure or protecting national security".[30]

BSA is concerned about the proposal to allow disclosure of protected information to all government entities "regardless of policy responsibility". As highlighted in our comments on Measure 3, protected information will be sensitive in nature and there should be safeguards to protect such information, including how and when such information is to be shared with other government entities. As with the limited use obligation, we recommend that that the Secretary of Home Affairs seek the affected entity's consent to share the information with other government entities, and in the process explain to the affected entity *why* the information has to be shared, and with *which* government entities. It also follows that there only relevant information should be shared, and that there are rigorous safeguards to protect such information from unauthorised access or disclosure, or from regulatory actions being taken against the information reporting organization.

<u>Recommendation 18</u>: Introduce requirements to seek the affected entity's consent before sharing protected information with other government entities, and ensure that there are adequate safeguards protecting such information from unauthorised access or disclosure.

Measure 8: Review and remedy powers

Measure 8 proposes to introduce a "formal, written directions power in Part 2A of the SOCI Act to address seriously deficient elements of a CIRMP".[31] The Consultation Paper observes that there is "currently no legislative framework which allows the regulator to issue a direction to an entity to remedy a deficient risk management program when a regulator assesses it as such and when the

---

[28] Consultation Paper (2023), p. 48-49.

[29] See: https://www.cisc.gov.au/how-we-support-industry/regulatory-obligations/protected-information#:~:text=%E2%80%8BThe%20Security%20of%20Critical,functions%20under%20the%20SOCI%20Act, accessed 7 February 2024.

[30] Consultation Paper (2023), p. 49.

[31] Consultation Paper (2023), p. 52.

entity is unwilling to comply with the regulator's recommendations", and this proposed power is intended to plug the perceived gap.[32]

The Government assumes that there will be situations where a CIRMP is so "seriously deficient" that it requires the Government to step in. This is arguably premature. Not all CIRMP-related obligations, notably the requirements for managing cyber and information hazards,[33] have entered into force. Critical infrastructure entities are also not yet obligated to submit their inaugural board-approved annual report until later this year.[34] The Consultation Paper also did not identify any actual events where the Government needed to rectify a seriously deficient CIRMP but was prevented from doing so because it did not have the requisite power. We recommend that the Government refrain from introducing yet another power, especially when CIRMP obligations are not yet fully operational and there is no evidence that the Government requires such a power.

Recommendation 19: Refrain from introducing a new review and remedy power, given that the CIRMP-related obligations are not yet fully operational and there is no clear evidence that the Government requires such a power.

Similar to our points above on Measure 6 (Consequence Management Powers), we note that there are no effective checks on this proposed power. Notably, the Government and the critical infrastructure entity may disagree on whether a CIRMP is deficient, or whether the actions taken to remedy any alleged deficiencies are sufficient.

In this regard, if the proposed power is implemented, we reiterate our earlier recommendations to define key terms (notably, "seriously deficient" and "material risk") to properly scope the exercise of the power, introduce independent oversight mechanisms and to allow for review of the Government's decision to exercise the power.

Recommendation 20: If introduced, define key terms (notably, "seriously deficient" and "material risk") to properly scope the exercise of the power, subject the power to independent oversight, and provide affected entities with the right to appeal/review the Government's exercise of the power.

Measure 9: Telecommunications sector security under the SOCI Act

Measure 9 proposes to "consolidate security regulation for the telecommunications sector under the SOCI Act", as this "commensurate with the criticality and risk profile of the telecommunications sector".[35]

BSA supports this proposed measure. We have consistently advocated on the importance of regulatory coherence and reducing complexity in the cyber security landscape, as doing so will improve understanding and compliance. This is a step in the right direction, and BSA encourages the Government to continue identifying opportunities to streamline and simplify complex (and oftentimes overlapping) cyber security requirements.

Recommendation 21: Consolidate security regulation for the telecommunications under the SOCI Act, and continue identifying opportunities to streamline and simplify complex cyber security requirements.

Conclusion

We hope that our comments will assist the Government in its legislative reform efforts. We look forward to serving as a resource as you continue to engage with industry.

Please do not hesitate to contact me if you have any questions regarding this submission or if I can be

[32] Consultation Paper (2023), p. 51.

[33] Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023, Section 8.

[34] SOCI Act, Section 30AG.

[35] Consultation Paper (2023), p. 54-55.

of further assistance.

Sincerely,

Tham Shen Hong
Senior Manager, Policy – APAC