25 October 2024

BSA COMMENTS ON CYBER SECURITY LEGISLATIVE PACKAGE 2024

Submitted Electronically to the Parliamentary Joint Committee on Intelligence and Security

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the Parliamentary Joint Committee on Intelligence and Security's (**PJCIS**) inquiry into the Cyber Security Legislative Package 2024, which consists of the *Cyber Security Bill 2024* (**Cyber Security Bill**), the *Intelligence Services and other Legislation Amendment (Cyber Security Bill) 2024* (**Intelligence Services Bill**), the *Security of Critical Infrastructure and Other Legislation Amendments (Enhanced Response and Prevention) Bill 2024* (**SOCI Act Amendment Bill**), as well as the accompanying Explanatory Memorandums.

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, network infrastructure services, cybersecurity solutions, and collaboration systems. 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.

BSA has participated in multiple consultations on the proposed cybersecurity legislative amendments.[2] While we support a majority of the amendments, we remain concerned about the following matters: a) when impacted entities provide authorities with sensitive information on an incident, the authorities are not expressly required to seek their consent for sharing it or explain why and with whom it will be shared; and b) there are still no independent oversight mechanisms over the exercise of various powers, notably those in Part 3A of the *Security of Critical Infrastructure Act 2018* (**SOCI Act**), which will increase in scope following the amendments.

Summary of BSA's Comments

Cyber Security Bill

1. **Secure by design standards for Internet-of-Things Devices:** Australia should recognise and accept other internationally recognised standards, such as the ISO/IEC 27402:2023

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Cohere, Dassault, Databricks, DocuSign, Dropbox, Elastic, ESTECO SpA, EY, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Notion, Okta, OpenAI, 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] BSA Comments on Cyber Security Legislative Reforms Consultation Paper, February 2024, https://www.bsa.org/files/policy-filings/02292024bsaaucybersec.pdf. BSA also filed a response to the Department of Home Affairs on 11 September 2024 following the Department's closed-door consultations on the reforms.

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

standard, and take every effort to avoid a divergent approach from other like-minded countries.

2. **Ransomware reporting obligations:** BSA supports: a) establishing a threshold of A$3 million for entities to make a ransomware report; b) folding the ransomware reporting requirement into the mandatory reporting obligations under Part 2B of the SOCI Act; and c) requiring a ransomware report to be made only after payment (and not upon receiving a demand). We also support establishing a clear nexus between a reporting business entity that received a ransomware demand and any entity that provides a payment pursuant to said demand.

3. **Coordination of major cyber security incidents**: BSA supports establishing a limited use obligation for information provided to the National Cyber Security Coordinator (**Coordinator**) by an entity impacted by the cyber security incident, and the voluntary nature of the information sharing provision. However, the Coordinator should be required to seek the impacted 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.

4. **Cyber Incident Review Board:** BSA welcomes the creation of the Cyber Incident Review Board (**CIRB**) and supports including an Expert Panel as part of the CIRB structure. We also support requirements for: a) the CIRB to consult with the impacted entity on potentially sensitive information within the draft report; b) the report to not identify any individual unless they have consented; and c) sensitive information to be redacted from the public review report. However, BSA does *no*t support vesting the CIRB with powers to compel entities to provide information. BSA further suggests that the CIRB communicate with similar entities in other countries, like the Cyber Safety Review Board in the United States (which notably does not possess subpoena authority) to ensure resources are maximised.

Intelligence Services Bill

5. **Limited use of information by the Australian Signals Directorate (ASD):** As with the proposed establishment of a limited use obligation for information provided to the Coordinator, BSA supports the same obligation in the context of the ASD, insofar as the information provided to the ASD only may be shared by the ASD for "permitted cyber security purposes". However, ASD should be required to seek the impacted 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.

SOCI Act Amendment Bill

6. **Data storage systems that hold business critical data:** BSA supports making clear that data storage systems that hold business critical data form part of a critical infrastructure asset.

7. **Managing consequences of impacts of incidents on critical infrastructure assets:** BSA supports this amendment to the extent that it does not introduce a new, broadly scoped power. We also support limiting intervention requests to cyber incidents. However, we remain concerned about the lack of an independent oversight mechanism over the exercise of the broad powers under Part 3A of the SOCI Act.

8. **Use and disclosure of protected information:** BSA supports requiring authorisation by the Secretary of Home Affairs before sharing protected information but further recommends 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.

9. **Direction to vary critical infrastructure risk management program:** BSA disagrees with the introduction of this "review and remedy" power. There is no clear evidence that the Government needs this power and we remain concerned about the lack of effective checks.

10. **Security regulation for the telecommunications sector:** BSA supports consolidating security requirements for critical telecommunications assets from Part 14 of the *Telecommunications Act 1997* (**Telecommunications Act**) into the SOCI Act.

Cyber Security Bill 2024

Security standards for Internet-of-Things devices

The Cyber Security Bill will allow the relevant Minister to "mandate security standards as Ministerial rules for smart devices".[3] BSA notes that implementing a mandatory standard in Australia goes beyond the approach of other countries that are considering or have developed a voluntary labelling scheme. In the spirit of interoperability and compatibility, and with the view of minimising regulatory burdens, we urge Australia to take every effort to avoid a divergent approach from other like-minded countries, and to also recognise and accept other internationally-recognised standards, such as the ISO/IEC 27402:2023 standard.

Ransomware reporting obligations

On the entities which the ransomware obligations would apply to, BSA supports establishing a threshold of A$3 million for entities to make a ransomware report. Ransomware attacks are more commonly experienced and have a more damaging impact on small and medium enterprises. As such, setting the threshold at A$3 million will not only substantially increase the sample size for collecting ransomware information, but also reinforce the importance of robust cybersecurity practices for all enterprises. This threshold is also aligned with the definition of "small business" in the *Privacy Act 1988*.[4]

BSA notes that the ransomware reporting requirement would also apply to all responsible entities for critical infrastructure assets required to report cyber security incidents under Part 2B of the SOCI Act.[5] We support this as it effectively folds the ransomware reporting requirement into the mandatory reporting obligations under Part 2B of the SOCI Act. This also makes clear that ransomware incidents would constitute malicious cyber activity that will trigger the reporting requirement in the SOCI Act, thus improving regulatory certainty for businesses.

BSA supports requiring a ransomware report to be made only after payment (and not upon receiving a demand). As currently drafted, the requirements which will trigger the ransomware reporting obligation apply cumulatively.[6] Relatedly, we welcome the clarification that "the obligation is enlivened if the reporting business entity provides or is aware that another entity has provided on their behalf, a payment or benefit (a ransomware payment) to the extorting entity that is directly related to the demand" [emphasis added].[7] This creates a clear nexus between a reporting business entity that

[3] Explanatory Memo on Cyber Security Bill 2024, October 2024, p.3.

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

[5] Explanatory Memo on Cyber Security Bill 2024, p. 5.

[6] Cyber Security Bill 2024, p. 28. The ransomware obligation applies if: "(a) an incident has occurred, is occurring or is imminent; and (b) the incident is a cyber security incident; and c) the incident has had, is having, or is likely to have, a direct or indirect impact on a reporting business entity; and (d) an entity (the extorting entity) makes a demand of the reporting business entity, or any other entity, in order to benefit from the incident or the impact on the reporting business entity; and (e) the reporting business entity provides, or is aware that another entity has provided on their behalf, a payment or benefit (a ransomware payment) to the extorting entity that is directly related to the demand".

[7] Explanatory Memo on Cyber Security Bill 2024, p.40.

received a ransomware demand and any entity that provides a payment pursuant to said demand, thus reducing uncertainty for businesses.

Coordination of major cyber security incidents

BSA supports establishing a limited use obligation for information provided to the Coordinator by an entity impacted by the cyber security incident.[8] We appreciate that this limited use obligation is intended to "ensure that another government agency that has received this information can only use the information for the purpose for which it has been shared", which are limited to a series of "permitted cyber security purposes" as set out in the Cyber Security Bill.[9] Limiting and specifying the purposes that such information can be used for will further encourage industry stakeholders to provide information to the Coordinator.

Relatedly, BSA also supports the voluntary nature of the information sharing provision, which expressly states that the "[i]mpacted entity may voluntarily provide information to [the] National Cyber Security Coordinator in relation to a major cyber security incident".[10]

However, BSA also notes that most, if not all, of the information shared by the impacted entity with the Coordinator will be sensitive in nature. In addition, the impacted entity may not know how its information is being used, and which agencies are privy to it. In this regard, the Cyber Security Bill should require the Coordinator to seek the impacted 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. This will provide industry stakeholders with more visibility into how their information is being handled and engender greater trust between industry and the Government, which is critical for facilitating timely responses to incidents and uplifting cyber security.

Cyber Incident Review Board

BSA welcomes the creation of the CIRB. We are especially supportive of the inclusion of an Expert Panel in the CIRB structure, which will consist of a "pool of industry experts with high levels of cyber security, legal or sectoral expertise and experience".[11] Many BSA members operate in multiple markets and invest enormous resources in their own cyber security capabilities, which 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.

However, BSA is *not* supportive of vesting the CIRB with powers to compel entities to provide information.[12] There may be circumstances where a company representative is invited to be part of an Expert Panel tasked with reviewing an incident involving the company's competitor.[13] The ability to require the competitor to disclose sensitive information is especially concerning. Furthermore, the information gathering powers are essentially self-judging – the Board itself is responsible for assessing, among other things, if an entity "has a document that is relevant to the review"[14] and that

[8] Explanatory Memo on Cyber Security Bill 2024, p. 6.

[9] Explanatory Memo on Cyber Security Bill 2024, p. 7 and Cyber Security Bill 2024, p. 10 and 43.

[10] Cyber Security Bill 2024, p. 40.

[11] Explanatory Memo on Cyber Security Bill 2024, p. 8.

[12] Cyber Security Bill 2024, p. 56.

[13] BSA notes that Subsection 70(5) of the Cyber Security Bill only provides for a rule making power "to make provisions for or in relation to the Expert Panel for the membership of the Expert Panel, appointment of members to the Expert Panel, appointments of its members to a review panel for a review, terms of appointment of members, remuneration of members, resignation of members, disclosure of interests by members, termination of appointment of members and leave of absence for members". It is therefore unclear how conflicts of interests will be resolved.

[14] Cyber Security Bill 2024, p. 56.

any previously provided information "was not provided to the extent requested".[15] The entity that is subject to such powers will also have no avenue of recourse or appeal.

The CIRB will also be tasked with preparing a report detailing recommendations and the reason for those recommendations. We support requirements for: a) the CIRB to consult with the impacted entity on potentially sensitive information within the draft report; b) the report to not identify any individual unless they have consented; and c) sensitive information to be redacted from the public review report.

Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024

Limited use of information by the Australian Signals Directorate

As with the proposed establishment of a limited use obligation for information provided to the Coordinator, BSA is supportive of the same obligation in the context of the ASD, insofar as the information provided to the ASD[16] may only be shared by the ASD for "permitted cyber security purposes".[17]

However, we also reiterate our earlier recommendation that, if ASD intends to share the information provided to it by an impacted entity, ASD should be required to seek the impacted 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.

Security of Critical Infrastructure and Other Legislation Amendments (Enhanced Response and Prevention) Bill 2024

Data storage systems that hold business critical data

BSA supports the proposed amendments in this section, which have the effect of making clear that data storage systems that hold business critical data form part of a critical infrastructure asset. Importantly, we note that the amendments do not impose direct obligations on service providers which are further down the cyber security "chain" (i.e., service providers supporting a critical infrastructure entity). This is crucial as it continues to reflect the distinct roles and responsibilities of different actors along the "chain", and avoids creating unnecessary regulatory complexity.

Managing consequences of impacts of incidents on critical infrastructure assets

BSA previously expressed concerns regarding the necessity of introducing new consequence management powers and the potentially broad scope of such powers. In this regard, we note that instead of introducing an entirely new section vesting the Government with such powers, the SOCI Act Amendment Bill expanded the existing government assistance framework under Part 3A of the SOCI Act, by substituting the phrase "cyber security incident" with "an incident" or "an incident that has had, is having, or is likely to have, a relevant impact on one more critical infrastructure assets" throughout Part 3A.[18]

---

[15] Explanatory Memo on Cyber Security Bill 2024, p. 74.

[16] In this regard, BSA notes that, as set out in p.4 of the Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024, the information captured under the limited use obligation would have to relate to a cyber security incident that has occurred, is occurring, or a cyber security incident that may potentially occur, and been: a) voluntarily provided to, ASD by the impacted entity or another entity acting on behalf of the affected entity, such as an incident response provider; or b) acquired or prepared by ASD with the consent of the impacted entity, or c) disclosed to ASD by the National Cyber Security Coordinator under their limited use obligation within the Cyber Security Bill 2024.

[17] Intelligence Services and Other Legislation Amendment (Cyber Security) Bill 2024, p. 6.

[18] SOCI Act Amendment Bill 2024, p. 6.

BSA supports this amendment to the extent that it does not introduce a new, broadly-scoped power. We also support limiting intervention requests[19] to cyber incidents – as rightly noted in the Explanatory Memo, the acts that may be specified in an intervention request "would not be appropriate in responding to non-cyber incidents, like natural disasters".[20]

However, we continue to be concerned about the lack of an independent oversight mechanism. Notwithstanding existing safeguards set out in sections 35AB and 35AD of the SOCI Act, the fact remains that they only require the relevant Minister to consult within the Government and the affected entity before exercising these broad powers, which now apply to situations beyond cyber incidents. 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**).

As such, we reiterate our recommendation to implement additional independent oversight mechanisms to prevent the misuse of such discretion, and to allow for legislative appeal or review of the 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.

Use and disclosure of protected information

BSA supports requiring authorisation by the Secretary of Home Affairs before sharing protected information.[21] As highlighted above, protected information will be sensitive in nature and there should be safeguards to limit the sharing of such information. As with our comments on 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. As noted in the Explanatory Memo, such clarity will "provide entities confidence in [the Government's] use and disclosure of personal information, limit disruption and undue burden of the regulatory framework on entities and facilitate broader security uplift by facilitating appropriate collaboration between industry and Government".[22]

Direction to vary critical infrastructure risk management program

BSA disagrees with the introduction of this "review and remedy" power. The Government assumes that there will be situations where a Critical Infrastructure Risk Management Program (**CIRMP**) is so "seriously deficient" that it requires the Government to step in. This is premature. The requirements for managing cyber and information hazards[23] have just entered into force in August 2024, and critical infrastructure entities would have just submitted their inaugural board-approved annual report in September 2024. As such, there is no clear evidence that the Government requires such a power.

In addition, similar to our comments on proposed amendments to expand the powers under Part 3A of the SOCI Act, we are concerned that there are no effective checks on this proposed "review and remedy" power. The key terms scoping the exercise of this power, notably "serious deficiency" and "material risk",[24] are too vague and do not give a clear indication of when this power may be invoked. Furthermore, the Government and the entity may disagree on whether a CIRMP is deficient, or whether the actions taken to remedy any alleged deficiencies are sufficient.

---

[19] Per the Explanatory Memo on the SOCI Act Amendment Bill 2024, p.11, we understand "intervention requests" to be requests to authorise the ASD to do the types of things specified in section 35AC of the SOCI Act, which including to access or modify computers in order to resolve a cyber incident.

[20] Explanatory Memo on the SOCI Act Amendment Bill 2024, p.11.

[21] SOCI Act Amendment Bill 2024, p. 19.

[22] Explanatory Memo on the SOCI Act Amendment Bill 2024, p. 23.

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

[24] SOCI Act Amendment Bill 2024, p. 22.

Security regulation for the telecommunications sector

BSA supports consolidating security requirements for critical telecommunications assets from Part 14 of the Telecommunications Act into the SOCI Act. 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.

Conclusion

We hope that our comments will assist the PJCIS with its inquiry. 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 of further assistance.

Sincerely,

[redacted]

Tham Shen Hong
Senior Manager, Policy – APAC