28 February 2022

BSA SUBMISSION TO THE PJCIS REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE PROTECTION) BILL 2022

Submitted Electronically to the Parliamentary Joint Committee on Intelligence and Security

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to contribute to the review by the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) into the proposed *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*[2] (**Bill Two**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernise and grow. Many of BSA's member companies have made significant investments in Australia, and we are proud that many Australian organisations and consumers continue to rely on our members' products and services to support Australia's economy. BSA previously provided comments on Australia's critical infrastructure (**CI**) protection legislation.[3]

BSA thanks the PJCIS for this opportunity to comment and for the Committee's efforts to enhance CI protection legislation in Australia through its *Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*[4] (**Advisory Report**). Protecting CI is a critically important priority for Australia and BSA fully supports the Government's efforts to update its CI protection regime.

---

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fr6833%22

[3] See:

- **a)** BSA Response to Critical Infrastructure Consultation Paper, September 2020, https://www.bsa.org/policy-filings/australia-bsa-response-to-critical-infrastructure-consultation-paper (**BSA Sep 2020 Submission**);
- **b)** Critical Infrastructure Bill – BSA Comments, November 2020, https://www.bsa.org/policy-filings/australia-bsa-comments-on-australian-critical-infrastructure-bill-consultation (**BSA Nov 2020 Submission**);
- **c)** BSA Submission to the PJCIS Review of the Security Legislation Amendment (Critical Infrastructure Bill) 2020, Feb 2021, https://www.bsa.org/policy-filings/australia-bsa-submission-to-the-pjcis-review-of-the-security-legislation-amendment-critical-infrastructure-bill-2020 (**BSA Feb 2021 Submission**); and
- **d)** BSA Comments on Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, January 2022, https://www.bsa.org/policy-filings/australia-bsa-comments-on-security-legislation-amendment-critical-infrastructure-protection-bill-2022 (**BSA Jan 2022 Submission**).

[4] Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/SOCI/Report

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

BSA appreciates the inclusive and wide-ranging industry engagement undertaken by the Department of Home Affairs (**DHA**) to consult on the rules underpinning the Risk Management Program (**RMP**) and on the Exposure Draft of Bill Two, and acknowledges the changes that have been made to Bill Two prior to its introduction to Parliament in response to industry feedback.

While a number of BSA's previous concerns have been addressed by DHA through this process, BSA retains several concerns with Bill Two and kindly request that the PJCIS address these through its recommended amendments. Additionally, BSA retains one key concern with the *Security Legislation Amendment (Critical Infrastructure) Bill 2021* (**Bill One**) and, pursuant to Recommendation 8 of the PJCIS Advisory Report,[5] request the Committee considers this as part of its concurrent review of the operation to date of Bill One.

BSA recognises the short timeframe in which the PJCIS must complete the review and has focused its submission around five key recommendations that, if implemented, would improve security and build resilience in Australia's CI sectors, while reducing unnecessary and counter-productive obligations.

Summary of BSA's Recommendations

- Provide the right to request, but not the authority to compel, the installation of software in Systems of National Significance (SONS), exempt SONS operators from liability arising from disruptions or other problems caused by the installed software, and indemnify SONS operators from any losses that occur due to the installation of software.

- Implement strict safeguards and oversight mechanisms, including independent authorisation and review of determinations to request or require information. If the authority to compel software installation in SONS is maintained, there should be, at the minimum, 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.

- Set out legal processes to guide the exercise of powers to compel information sharing or the installation of software. For example, the information shared or collected should be used only for cybersecurity purposes or for limited law enforcement activities against malicious cyber actors.

- Define the rights and obligations of CI operators that are not themselves designated SONS, but have enterprise end-users that are designated SONS.

- Amend the notification period from 12 hours to 72 hours when a reportable critical cyber security incident is occurring, and to allow CI operators to follow-up with a written report "as soon as practicable".

Recommendation 1: Provide only the right to request installation of software in SONS, and protect SONS from associated liabilities

BSA strongly objects to the proposed power to compel the installation of software that transmits system information to the Australian Signals Directorate (**ASD**), potentially against the wishes and advice of the SONS operator.[6] Further, any collection of information under such an arrangement

[5] PJCIS Advisory Report, Recommendation 8 – "Once reintroduced, Bill Two should be referred to the Parliamentary Joint Committee on Intelligence and Security for review, with a **concurrent review of the operation to date of the amendments to the *Security of Critical Infrastructure Act 2018* resulting from Bill One**" [emphasis added].

[6] Bill Two, Division 5 Subdivision B – System information software

should also be appropriately limited such that customer content (including that of an overseas customer using an Australia-based service) are excluded to avoid conflicts with privacy law, contractual obligations, breach notification or other legal requirements of other jurisdictions.

While Part 3A of Bill One also allows the Minister for Home Affairs to authorise the ASD to install a computer program in a CI asset when a cyber security incident has taken place,[7] that power may only be invoked as part of the Government's incident response to serious cyber security incidents and will last only as long as the period specified in the Minister's authorisation.[8] Except for the requirement that a systems information notice cannot be longer than 12 months,[9] Bill Two does not specify similar limitations in respect of the proposed power to compel the installation of software. Introducing any software or new capability into enterprise IT systems, especially on a persistent basis, should only be done following a rigorous change management process to mitigate the risk to the security and stability of the network systems. Even though Bill Two requires the Secretary of Home Affairs (**Secretary**) to consult the responsible entity for the SONS before issuing a system information software notice,[10] there are no guidelines stipulating how thorough the consultation process should be. In particular, while the consultation process requires the Secretary to consider if the entity is technically capable of providing a report under sections 30DB or 30DC, as well as the costs associated with their compliance, it does not require the Secretary to consider the *effects* that any potential software installation may have on the SONS. As such, the Secretary could require software to be introduced into highly complex CI systems without adequate testing or vetting by SONS staff, or knowledge of the asset and its interdependencies. Moreover, mandatory installation of government software on enterprise systems can compromise users' confidence in the integrity and trustworthiness of the service provider's products and services, undermining their commercial competitiveness. This is particularly critical for cloud service providers (**CSPs**), where installing untested and thus potentially unsuitable software on global infrastructure puts enormous investments at risk for both the CSP and its enterprise customers. Such additional software to be installed within the boundary of the CSP system should be subject to the same transparency and security requirements of other software of the CSP (e.g., in relation to secure development practices, vulnerability management, software bill of materials).

BSA therefore recommends that Bill Two should only provide the Government with the right to request but not the authority to compel the installation of software in SONS. In addition, as such software may pose a risk to the stability of SONS' network systems, Bill Two should expressly exempt SONS operators from any liability arising from any malfunctions or problems caused by the installed software and indemnify the SONS operator from any losses that occur due to the installation of software.

Recommendations 2 and 3: Independent authorisation / review and legal processes to guide exercise of access powers

More generally, BSA is concerned with the authority vested in the Secretary to require SONS operators to provide access to system information.[11] Specifically, the provisions authorise the Secretary to demand access to system information via periodic or event-based reporting and require the Secretary to provide written notice[12] and consult with the responsible entities.[13] BSA is especially

[7] Bill One, Section 35AC(c).

[8] Bill One, Section 35AG.

[9] Bill Two, Section 30DL

[10] Bill Two, Section 30DK.

[11] Bill Two, Division 5 — Access to system information.

[12] Bill Two, Section 30DB and 30DC, respectively.

[13] Bill Two, Section 30DD.

concerned that there appears to be no independent oversight mechanisms expressly specified in Bill Two in respect of these extraordinary powers. The only apparent limitation on the Secretary's discretion is that the Secretary must have regard to "the costs that are likely to be incurred by the entity in complying with the notice" and "such other matters (if any) as the Secretary considers relevant."[14]

BSA encourages implementing additional independent oversight mechanisms to prevent the misuse of such discretion and to ensure that the act of compelling access to system information is used by the Government only in extreme situations. Further, if the authority to compel software installation in SONS is maintained, there should be, at the minimum, **a mandatory review process by an independent body of experts to assess the security, technical feasibility, and reasonableness of installing such software.** This is because such requests related to software installation risk serious interference with the normal operation and security of the network and potential reputational harm to a service provider. In this regard, BSA also supports the recommendation of the PJCIS to "formulat[e] a merits review system of appeal to the security division of the AAT for any determination under Bill Two for declarations under proposed Part 6A and proposed Part 2C, once revised, with requisite access to protected information."[15]

Bill Two should also expressly set out legal processes to guide the exercise of the access powers. BSA proposes the following:

- Compelled information sharing by the private sector with the Government should be strictly limited to information related to Australian assets and where Australian business critical data is processed. In the case of CSPs, such information should only be shared with the full knowledge and concurrence of the customer the data relates to.

- All shared information under this scheme relating to the CI operator should be treated as highly sensitive data and explicitly exempt from freedom of information requests and other data release schemes. It should only be used for cybersecurity purposes or for limited law enforcement activities against malicious cyber actors and should be attributable only with the permission of the sharing organisation.

Recommendation 4: Rights and obligations when enterprise end-users are designated SONS

Bill Two does not provide clear guidance on the rights and obligations of CI operators that are not themselves designated SONS but have enterprise end-users that are designated SONS.
This is particularly problematic in the context of the data storage/processing sector and specifically CSPs, as CSPs have a different relationship with their enterprise customers compared to operators from other CI sectors. Unlike in other CI sectors, the responsibility for cloud security is often shared between an enterprise end-user and their CSP. This "shared responsibility" security model is a very important principle of cloud security, and a lack of clarity in obligations could undermine the existing security arrangement between CSP and their SONS end-users. For example, the ASD may install a software in a SONS end-user to transmit system information periodically to ASD. However, the data processing service that a CSP is providing to the same SONS end-user may interfere with ASD's software, or vice versa. In such a situation, it is not clear if the CSP has obligations to ensure that its service would not interfere with ASD's software. It is also not clear if the CSP can be compelled to

[14] Bill Two, Sections 30DB(4) and 30DC(4).

[15] Advisory Report on the Security Legislation Amendment (Critical Infrastructure Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018, September 2021, at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024715/toc_pdf/AdvisoryreportontheSecurityLegislationAmendment(CriticalInfrastructure)Bill2020andStatutoryReviewoftheSecurityofCriticalInfrastructureAct2018.pdf;fileType=application%2Fpdf , para 3.49.

modify its services to accommodate ASD's software, since the CSP is not a designated SONS. Nor is it clear whether the CSP has any recourse to appeal or reverse a decision to install software on a SONS end-user's system that may interfere with the CSP's services.

BSA recommends that the DHA make clear the rights and obligations of CI operators that are not themselves designated SONS but have end-users that are designated SONS. For example, when enhanced cyber security obligations are imposed on a SONS, DHA should consult with all CI operators providing services to the SONS to determine if the enhanced cyber security obligations will affect the provisions of their services to the SONS. The DHA should also develop and publish guidance materials to assist CI operators in navigating their rights and obligations when their end-users are designated SONS.

Recommendation 5: Extend notification period for cyber security incidents

Under Bill One, where a CI operator becomes aware that a cyber security incident is occurring or has occurred, and the incident has had, or is having, a significant impact on the availability of the CI asset, the entity is required to report this incident either orally or in writing within 12 hours.[16] Where an oral report has been made, the CI operator must follow up by submitting a written record of the report within 84 hours of making the oral report.[17]

As with mandatory data breach reporting in the privacy context, BSA supports limited, tailored, and reasonable reporting requirements for CI operators where a cybersecurity incident results in a significant impact on the availability of the asset or a critical impact on the operation of CI operators within Australia. However, BSA is concerned with the short reporting timelines required under Bill One, as they potentially may divert the limited resources of security teams from the critical job of response. In the event of a truly significant incident, the attention and resources of a CI operator, and that of their data storage or processing providers, should be focused on detecting and responding to the incident. Shorter reporting timelines may also lead to reporting inaccurate or inadequately contextualised information, which is unhelpful for regulators and consequently counterproductive to cybersecurity response. Longer and more flexible reporting timelines also accord with international norms. For example, the *EU Directive on Security of Network and Information Systems* (**NIS Directive**), which also contains a cybersecurity breach reporting requirement, requires organisations to notify incidents "without undue delay". Businesses have the flexibility to focus their resources on responding to the incident before submitting a full report, and may choose to provide a preliminary notification of the incident and follow up with further details as investigation progresses. In the United States, while the *National Defense Authorization Act for Fiscal Year 2022* (**NDAA**) excluded cybersecurity incident reporting requirements, previous versions of the Act included a requirement to report cybersecurity incidents within 72 hours of confirming the incident's occurrence.[18]

BSA therefore recommends amending the notification period from 12 hours to 72 hours when a reportable serious incident is occurring, and to allow CI operators to follow-up with a written report "as soon as practicable". In addition to allowing more time for adequate incident investigation, this would also align the incident reporting obligations with the language used in the *Privacy Act 1988* on notifiable data breaches,[19] and with the practices of other important jurisdictions. Where the incident is particularly significant and quicker reporting will not impede remediation, responsible companies may also provide the relevant information sooner.

---

[16] Security Legislation Amendment (Critical Infrastructure) Act 2021, Section 30BC(1).

[17] Security Legislation Amendment (Critical Infrastructure) Act 2021, Section 30BC(3).

[18] Cyber Incident Reporting for Critical Infrastructure Act of 2021, which was subsequently added to the NDAA. See Sec 2220A (d)(5)(A)(i), https://www.congress.gov/bill/117th-congress/house-bill/5440/text.

[19] Privacy Act 1988 at https://www.legislation.gov.au/Details/C2021C00452, Section 26WK.

This is more flexible than imposing a rule for a shorter notification period and accommodates the varying circumstances that companies may face when reporting serious cyber incidents.

Conclusion

We thank the PJCIS for the opportunity to contribute to the review into the proposed Bill Two and appreciate the Committee's consideration of our above comments. We hope that our concerns and recommendations will assist in the development of enduring solutions to address the security of critical infrastructure in Australia. 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
Manager, Policy – APAC