31 January 2022

BSA COMMENTS ON SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE PROTECTION) BILL 2022

Submitted Electronically to the Department of Home Affairs

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to provide comments to the Department of Home Affairs (**DHA**) on the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (**Bill Two**) Exposure Draft[2] and its associated Explanatory Paper.[3]

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 has previously provided comments on Australia's critical infrastructure (**CI**) protection legislation.[4]

Following the enactment of the *Security Legislation Amendment (Critical Infrastructure) Bill 2021* (**Bill One**), which was passed by Parliament and received Royal Assent in December 2021, Bill Two establishes a Risk Management Program (**RMP**),[5] declarations of systems of national significance (**SONS**),[6] and enhanced cyber security obligations for operators of SONS, including the authority to require such systems to install software that transmits system information to the Australian Signals

[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] Exposure Draft, Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, December 2021, https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-Infrastructure-bill-2020.pdf.

[3] Explanatory Paper, Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, December 2021, https://www.homeaffairs.gov.au/reports-and-pubs/files/explanatory-document-SLACIP.pdf.

[4] 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**); and
- **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**).

[5] Exposure Draft (2021), Part 2A – Critical infrastructure risk management program.

[6] Exposure Draft (2021), Part 6A – Declaration of systems of national significance by the Minister. Systems of National Significance are critical infrastructure assets designated by the Minister due to the assets' importance to Australia's national security, defence, or social or economic stability.

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

Directorate (**ASD**).[7] Bill Two also proposes amendments to key sector and asset definitions which were introduced in Bill One.[8]

While many of these reforms may improve security and build resilience in Australia's CI sectors, Bill Two would be further improved by implementing the following recommendations. These recommendations are designed to make clear the scope of the requirements, 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 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 who are not themselves designated SONS, but with end-users who are designated SONS.

- Amend the definition of "critical data storage or processing asset" such that the "business critical data" threshold also applies to assets provided to the government entities listed in Section 12F(1)(b).

- Extend the grace period for businesses to bring their practices in line with the applicable RMPs rules from six months to 12 months.

- 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".

Enhanced Cyber Security Obligations

Bill Two proposes to impose enhanced cyber security obligations on CI operators designated as SONS.[9]

BSA is concerned with the obligation to provide access to system information,[10] through which the Secretary of the DHA (**Secretary**) may require the SONS operator to provide access to system

[7] Exposure Draft (2021), Part 2C – Enhanced cyber security obligations.

[8] Explanatory Paper (2021), para 20.

[9] Explanatory Paper (2021), para 86.

[10] Explanatory Paper (2021), para 116.

information through periodic reporting requirements to the ASD.[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 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 should be used by the Government only in extreme situations.

BSA also strongly objects to the proposed power to compel the installation of software that transmits system information to ASD, potentially against the wishes and advice of the SONS operator. 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,[15] 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.[16] Bill Two, in contrast, does not specify such 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. As proposed under Bill Two, the Secretary could require software to be introduced into highly complex CI systems without adequate testing or vetting by company 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.

In view of our concerns above, BSA recommends the following:

- **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.

- **Bill Two should 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, 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 Parliamentary Joint Committee on Intelligence and

[11] Exposure Draft (2021), Division 5 — Access to system information.

[12] Exposure Draft (2021), Section 30DB and 30DC, respectively.

[13] Exposure Draft (2021), Section 30DD.

[14] Exposure Draft (2021), Sections 30DB(4) and 30DC(4).

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

[16] Bill One, Section 35AG.

Security (**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*".[17]

- For transparency, Bill Two should expressly require the ASD to provide a Software Bill of Materials (**SBOM**) whenever it installs software in a SONS. This would allow SONS to better explain to their end-users the contents of the installed software, and to address any concerns their end-users may have.

- **Bill Two should expressly set out legal processes to guide the exercise of access powers.** BSA proposes the following:
    - Information sharing by the private sector with the Government should be strictly limited to information related to Australian assets and where 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.

Rights and Obligations When 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 end-users who 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 customers compared to operators from other CI sectors. Unlike in other CI sectors, the responsibility for cloud security is often shared between an 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 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.

[17] 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.

Key Sector and Asset Definitions — Critical Data Storage or Processing Asset

The proposed amended definitions to "data storage or processing services" and "critical data storage or processing asset" are an improvement over those adopted in Bill One. Specifically, we note that the amended definition of critical storage or processing asset will make clearer the type of entities that will be captured as responsible entities for these assets. However, this definition could be further improved by limiting it to assets managing "business critical data", even when the asset is being provided to the government entities.

In brief, Section 12F of Bill One sets out two situations where an asset is considered a "critical data storage or processing asset". The first situation, set out in Section 12F(1), is where the asset is used to provide a data storage or processing service to the Government and its associated entities. The second situation, set out in Section 12(F)(2), is where the asset is used to provide a data storage or processing service to an entity responsible for a CI asset and "relates to business critical data".[18] **The requirement for the asset to relate to business critical data should apply to both situations above.** Within organisations, not all assets, systems, networks, data, and services are equally important or essential. CI policies should avoid overreaching and imposing compliance burdens where they are not necessary. Treating non-critical systems in the same way as those that are truly critical risks misallocating limited security resources.

As such, BSA recommends amending Section 12F(1) such that the "business critical data" threshold also applies to critical data storage or processing assets provided to government entities, as follows:

12F Meaning of *critical data storage or processing asset*

(1) An asset is a critical data storage or processing asset if:
- (a) it is owned or operated by an entity that is a data storage or processing provider; and
- (b) it is used wholly or primarily to provide a data storage or processing service that is provided by the entity on a commercial basis to an end-user that is:
  - (i). the Commonwealth; or
  - (ii). a body corporate established by a law of the Commonwealth; or
  - (iii). a State; or
  - (iv). a body corporate established by a law of a State; or
  - (v). a Territory; or
  - (vi). a body corporate established by a law of a Territory; ~~and~~
- (c) **relates to business critical data;**
- (d) the entity knows that the asset is used as described in paragraph**s** (b) **and (c)**; and
- (e) the asset is not a critical telecommunications asset.

In determining what type of information would fall within the threshold of "business critical data" in a government setting, a ready-made solution is available through the assessment of the sensitivity of government information utilising the Business Impact Level tool in the Australian Government's Protective Security Policy Framework.[19] BSA suggests imposing a business critical data threshold of

[18] Security Legislation Amendment (Critical Infrastructure Protection) Act 2021 at https://www.legislation.gov.au/Details/C2021A00124. Section 5, "**business critical data** means: (a) personal information (within the meaning of the Privacy Act 1988) that relates to at least 20,000 individuals; or (b) information relating to any research and development in relation to a critical infrastructure asset; or (c) information relating to any systems needed to operate a critical infrastructure asset; or (d) information needed to operate a critical infrastructure asset; or (e) information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset."

[19] Australian Government Protective Security Policy Framework, Policy 8: Sensitive and classified information, https://www.protectivesecurity.gov.au/system/files/2021-11/pspf-policy-8-sensitive-and-classified-information.pdf

Business Impact Level 2 (i.e., when the compromise of information confidentiality would cause limited damage to an individual, organisation, or government).

Risk Management Programs

BSA previously recommended that sector-specific rules should be risk-based and focused on driving desired security outcomes.[20] It is important to provide private sector entities the latitude to develop the most effective and innovative approaches to meet those security outcomes. Outcome-based approaches that integrate risk assessment tools, maturity models, and risk management processes enable organisations, including CI operators, to prioritise cybersecurity activities and make informed decisions about cybersecurity resource allocation and to align defences against the most pressing risks.

In this regard, we are encouraged to see that, as stated in the Explanatory Paper, CI operators have some flexibility to determine which risks are to be considered "material" and the appropriate measures to manage those risks.[21] The flexibility of this approach provides strong, repeatable security outcomes while accounting for the diversity and constant evolution within CI sectors in terms of technological infrastructure, types of risk, and threats and threat actors.

A possible area of improvement relates to the period for CI operators to bring their practices in line with the applicable RMP rules. While not expressly covered or stated in Bill Two, the Explanatory Paper acknowledges that bringing business practices into line with the RMP rules may take time and, as such, the RMP rules would have a "a six month delayed commencement as a minimum to allow an appropriate transition period."[22] This is also reflected in the draft RMP rules, which specify that responsible entities for CI assets must, within six months of the commencement of the rules, ensure that their RMPs meet certain requirements (e.g., in respect of Cyber and Information Security Hazards, the RMP would need to include details of "a risk-based plan that outlines strategies and security controls as to how cyber and information security threats are being mitigated").

However, six months is insufficient for CI operators to develop and implement a program that effectively identifies and mitigates all relevant material risks to their businesses. While CI operators have some flexibility in this regard, as acknowledged above, the RMP rules still require responsible entities to address risks in four specific domains, namely: a) physical security and natural hazards; b) cyber and information security hazards; c) personnel security hazards; and d) supply chain hazards.[23] This short timeframe means that CI operators will need to divert important resources, such as cybersecurity experts and teams, to expeditiously develop the RMP, concurrently with other pressing priorities related to complying with requirements from Bill One. This may result in fewer resources for CI operators to implement other compliance measures and address risks and hazards that will arise during this six-month period.

BSA recommends extending the period during which CI operators must develop and implement RMPs from six months to 12 months. This would give CI operators adequate time to bring their practices in line with the applicable RMPs rules responsibly.

---

[20] BSA Feb 2021 Submission, p. 5.

[21] Explanatory Paper (2021), para 69. However, BSA notes that businesses are required to consider certain specified factors when determining if a risk is a material risk, e.g., whether it may prejudice the social or economic stability of Australia and whether it would cause the stoppage or major slowdown of a critical infrastructure asset's functioning for an unmanageable period.

[22] Explanatory Paper (2021), para 52. This six-month period was also specified in the Draft Risk Management Program Rules, dated November 26, 2021.

[23] Explanatory Paper (2021), para 71.

Notification of 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.[24] 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.[25]

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 it may potentially 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, and notifying the impacted customers if appropriate. Shorter timelines may also lead to reporting of inaccurate or inadequately contextualised information, which are unhelpful for regulators and consequently counterproductive to cybersecurity response. Longer and more flexible 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 either focus their resources on responding to the incident before submitting a full report, or to provide a preliminary notification of the incident and follow up with further details as investigation progresses. In the US, 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.[26]

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,[27] and with the practices of other important jurisdictions.

Conclusion

We thank the DHA for the opportunity to comment on Bill Two. 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,

Tham Shen Hong

Tham Shen Hong
Manager, Policy – APAC

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

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

[26] 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.

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