12 February 2021

Parliamentary Joint Committee on Intelligence and Security

Submitted electronically

BSA SUBMISSION TO THE PJCIS REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020

BSA | The Software Alliance (**BSA**) appreciates 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) Bill 2020*[1] (the **Bill**) and the *Security of Critical Infrastructure Act 2018*[2] (the **Act**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[3] are among the world's most innovative companies, creating software solutions that spark the economy. Member companies have made significant investments in Australia and we are proud that many Australian organisations and consumers continue to rely on their products and services to support Australia's economy.

BSA affirms our interest in critical infrastructure (**CI**) protection legislation in Australia and thanks the Committee for this opportunity to comment. Protecting CI is a critically important priority for Australia and BSA fully supports the Government's efforts to update its CI protection regime. As in most countries, Australian CI operators are largely private sector entities, and we are particularly encouraged to see that the approach to CI protection in Australia promotes close public-private collaboration and attempts to reflect the needs and objectives of all stakeholders.

Recommendations

In 2020, BSA provided comments on CI protection to the Department of Home Affairs (**DHA**) on the *Protecting Critical Infrastructure and Systems of National Significance* discussion paper[4] and the subsequent consultation on the draft Bill.[5]

---

[1] Security Legislation Amendment (Critical Infrastructure) Bill 2020, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657

[2] Security of Critical Infrastructure Act 2018, https://www.legislation.gov.au/Details/C2018A00029

[3] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[4] BSA Response to Critical Infrastructure Paper, https://www.bsa.org/files/policy-filings/09162020auciresponse.pdf

[5] Critical Infrastructure Bill — BSA Comments, https://www.bsa.org/files/policy-filings/11272020auscritinfrastructure.pdf

300 Beach Road
#25-08 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

Following those submissions BSA retains several concerns with the Bill and we request that the PJCIS recommend that the Bill be amended to:

- Remove the proposal for a "Data Storage and Processing" CI sector.
- Establish a voluntary public-private partnership CI scheme with adequate incentives to drive participation by the relevant private sector stakeholders.
- Establish a critical cyber risk-based incident reporting mechanism that prioritises incident remediation and management over reporting requirements by making the reporting of low-level events voluntary, limiting the scope of reporting to those impacting Australia, and applying a two-step reporting mechanism for serious events.
- Recognise that cloud service providers (**CSPs**) and other data storage and processing providers, under the "shared responsibility" model, may not have sufficient information or be able to respond to particular Government requests or requirements, and ensure CSP customers, including CI operators, also report relevant incidents.
- Avoid undermining physical security by requiring the disclosure of data center locations.
- Develop the co-design process as soon as possible to allow for industry to better comment on the Bill and understand the full implications of what is being proposed. The co-design process should produce mutually agreed upon requirements that focus on risk-based, outcome focused, and technology neutral security outcomes for CI sectors.
- Make "system information" sharing voluntary and explicitly limited to information relating to the Australian CI regime. System information should be shared beyond the regulator only with customer concurrence. The Bill should limit CI operators' liability for sharing and receiving information under the scheme.
- Treat all shared information under this scheme related to the CI operator as highly sensitive data and explicitly exempt from FOI requests and other data release schemes. It should only be used for cyber security purposes or for limited law enforcement activities against malicious cyber actors and should only be attributable with the permission of the sharing organisation.
- Remove the ability of the Government to compel CI operators to install software on their systems and replace this authority with the ability to request such actions.
- Narrow the Government's ability to forcefully intervene via the proposed "step-in" powers to specific cases, such as where CI operators are prevented from acting due to contractual issues, and add appropriate oversight and due process mechanisms to these powers.

DETAILS

Proposed Data Storage or Processing Sector

BSA recommends that the proposal to define a "Data Storage or Processing" CI sector be removed from the Bill.

The proposed "Data Storage or Processing" (**DSP**) CI sector is quite different in nature from the other CI sectors put forward in the Bill. Unlike the other proposed CI sectors which represent established industry verticals, the proposed DSP sector is not an industry in itself. Instead, it represents a collection of different companies, technologies, and services that cut across the economy. Just one part of the proposed sector, CSPs, would be held to multiple overlapping Australian regulatory requirements as they serve customers from a broad swathe of industry verticals including sector

specific rules for all CI sectors and, in the case of government customers, the Australian Government's Information Security Registered Assessors Program (**IRAP**) certification.

CSPs are already regulated under numerous privacy, sector vertical, and individual customer requirements and, as noted above, government standards. They also voluntarily participate in cyber threat sharing activities. Adding a further layer of regulation adds overhead without increasing security outcomes for Australia.

Instead of adding a further layer of regulation on CSPs, the Government should make it clear that CI operators must ensure that any CSPs they use are willing to and capable of following their security requirements. These requirements include any CI sector-specific obligations with which the CI operators must comply.

Partnership with Industry

Instead of the proposed compliance-based approach, the Bill should create a voluntary public-private partnership CI scheme with adequate incentives to drive participation by the relevant private sector stakeholders.

BSA applauds the Government's desire to partner with industry on the protection of CI in Australia and is a strong proponent of government and industry working together to solve issues such as these.

In our experience effective public-private partnerships depend on long-term relationships between governments and the relevant private sector stakeholders, including in this case CI operators and CSPs, among others. Such partnerships are built on trust and mutual benefit and aim to reduce costs and risks while achieving the governments' goals by leveraging the capabilities of the private sector.

In cases where governments establish clearly structured partnerships with relevant private sector stakeholders to share cybersecurity information, legislation should enable the voluntary bi-directional sharing of information between the public and private sectors, including by limiting the liability of providers sharing information and protecting them from anti-trust concerns. In such cases, providers benefit from receiving timely threat information from the government, enabling them to improve their network defenses, while providing the government invaluable threat information from businesses across a wide range of sectors and threat environments. Such partnerships work well, cost less to operate, and are sustainable because they are voluntary, mutually beneficial, and clearly structured.

However, instead of taking this approach, the Bill grants extensive powers to the Government to compel private sector participation in the "partnership". Under the proposed arrangement, it is unclear what the benefit of participation for CSPs would be and whether there would be any protections or other incentives for cooperation with the Government beyond the existing arrangements.

The Government should establish a voluntary public-private partnership mechanism, introducing strong incentives, such as limitations on liability for sharing of threat data and two-way information sharing, for participation by the relevant private sector stakeholders.

Positive Security Obligation

Critical cyber incident reporting

The Bill should establish a critical cyber risk-based incident reporting mechanism that prioritises incident remediation and management over reporting requirements.

As with mandatory data breach reporting in the privacy context, BSA supports reporting requirements for CI where a data breach or similar incident results, or will likely result, in a significant impact on the availability of the asset or a critical impact on the operation of CI operators within Australia. As currently described, the mandatory reporting scheme is overly burdensome and risks distracting security personnel from the more important tasks of cyber security, remediating and managing incidents. Furthermore, CSPs' first obligation should be to report any incidents to the customer. The customer is then able to meet any reporting obligations they might have, including those under any CI sector specific requirements that may apply.

The Bill proposes two types of incidents that trigger reporting requirements. They are incidents that have a "significant impact" to customers and those that have a "relevant impact". This risk-based approach is a good way to differentiate different cyber security incidents based on impact. However, the definition of "relevant impact" in the Bill (section 8G), which has a mandatory reporting obligation attached to it, has no minimum threshold and neither definition specifically limits the reporting obligation to impacted customers that are within the scope of this regulation, or even to those under the jurisdiction of Australian law potentially making it an extraterritorial requirement.

Without a minimal threshold, the "relevant impact" reporting alone could encompass many thousands of minimal events a day. The Bill proposes that the CI operator provide a written report for every reportable event, thus creating a heavy burden for busy cyber security teams.

BSA recommends that the mandatory incident reporting requirement should be a risk-based significant impact test, encompassing either scale or impact on CI services in Australia. The scheme should then apply a voluntary, low-impact reporting requirement to events that occur at the lower "relevant impact" threshold to provide a more flexible incident reporting regime.

BSA further recommends the definitions be amended to limit the scope of affected customers under the reporting requirement to those located within Australia.

In the event of a truly significant incident, the attention and resources of a CI operator, and that of their CSPs, should be focused on diagnosing and remediating the incident, and working with the impacted customer to restore service.

Extremely short mandatory incident reporting times, as required under the Bill (12 hours for critical cyber security incidents and 24 hours for other cyber security incidents) divert the limited resources of security teams from the critical job of remediation. Additionally, for some serious events, while investigation of the cause is still ongoing, reporting in the "approved form", as suggested in sections 30BC and 30BD, may not be possible with incomplete information.

BSA recommends amending the incident reporting requirements to a two-step process allowing operators to immediately notify the regulator when a reportable serious incident is occurring and following up with written reporting "as soon as possible", allowing time for adequate incident investigation in line with provisions under the notifiable data breaches scheme (*Privacy Act 1988*).[6]

Finally, in the case of CSPs, under the shared responsibility model of security, they neither have the visibility of nor ability to act on incidents that occur in parts of the cloud service that are the responsibility of the customer or other third-party providers contracted by the customer. Incidents in these instances must be the responsibility of the customer to report and it is inappropriate to apply penalties to CSPs in these cases.

BSA recommends that CSPs report incidents to their customers, and that customers then have an obligation to report to the Government. However, should the Government establish a DSP CI sector, mandatory incident reporting obligations for CSPs should be limited to those within CSPs' control.

Ownership reporting obligation

BSA supports requiring CI operators to report the ownership structure of the company and business office locations to governments for contact purposes. However, governments should not require disclosure of the exact location of data centres.

The location of data centres is closely held even within companies for physical security reasons. Sharing this data, no matter the good intention, undermines the physical security of these assets, and under an all-hazards approach to security risk, is not a detail that governments should force providers to share.

BSA recommends eliminating the requirement to provide data centre location information, and that asset owners instead be allowed to voluntarily provide this information after conducting an assessment of the risk to the asset. Furthermore, if provided information on data centre locations

[6] Privacy Act 1988, https://www.legislation.gov.au/details/c2014c00076

should be treated as sensitive information and explicitly exempt from FOI and other information requests.

Sector specific rules

The success of the Bill will depend, in part, on how the as-yet unknown co-design process for sector specific rules will work and be maintained into the future. As this process is still unknown, it is difficult for industry to provide effective comments on the efficacy and impact of the proposed CI protection regime. How the sector specific rules are developed is increasingly important in sectors in which the Government has little experience or expertise, such as in operating large scale CSP operations.

That said, there are a number of approaches and considerations that the Government could take in designing the Government-industry co-design process to achieve better CI security outcomes.

Every effort should be made to keep sector specific rules risk-based and centred on widely adopted and internationally recognised standards. Sector specific rules should focus security policies on driving desired security outcomes, providing private sector entities 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 to prioritise cybersecurity activities and make informed decisions about cybersecurity resource allocation and to align defences against the most pressing risks.

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. It also reduces the regulatory burden and takes advantage of existing workforce training pathways and technical standard maintenance processes.

Overly directive or prescriptive regulations focusing on strict compliance with specific methods or mandates that limit the use of security-enhancing technologies such as encryption can inhibit adaptive security measures and stifle innovation of new technologies.

The co-design process should produce mutually agreed upon requirements that focus on risk-based, outcome focused and technology neutral security outcomes for the sector. Both Government and industry must be able to agree on the requirements for sector specific rules to be fully successful. As part of this, the process should consider how to successfully mediate disagreements between participants and how to ensure that all participants are treated equitably, given adequate ability to participate, including those with specialist staff located overseas, and not subject to unfair, anticompetitive actions by other sector members.

BSA recommends that the co-design process be developed as soon as possible to allow industry to better comment on the Bill and understand its full implications.

Enhanced security obligations

Sharing “system information”

As with incident reporting policies, information sharing policies are most effective when they empower private entities to voluntarily share information regarding cybersecurity threat indicators with other private entities or governments. Such policies should expressly limit potential legal liability or regulatory consequences for both sharing and receiving information. Similarly, organisations should not be held liable for choosing not to share information with other private entities or governments outside of commercial vendor-customer relationships.

Information sharing by the private sector with the Government should also be strictly limited to data related to Australian assets and, in the case of CSPs, such information should only be shared with the full knowledge and concurrence of the customer the data relates to.

As such, BSA recommends that the Bill make clear that sharing “system information” is voluntary and any requirements to share such information must be explicitly limited to information relating to the Australian CI regime. The Bill should limit CI operators’ liability for sharing and receiving information under the scheme and information shared by CI operators should be shared beyond the regulator only

with customer concurrence. BSA also notes that there could be great utility to participants in a voluntary Australian technical information sharing network scheme among CSPs and other CI players.

The Government should take steps to reduce the risk to CI operators from loss of control and misuse of information shared under this scheme. The Bill proposes providing Government access to sensitive company system information which, if lost or uncontrolled, could allow malicious cyber actors to cause them significant damage, and subsequent financial damage. Such data should be protected at an extremely high level. Information sharing policies should ensure information shared under this scheme is used by the recipient only for cyber security purposes or to prosecute cyber criminals, and is not attributable without the provider's permission.

The Bill, except for a vague requirement to take a company's views into consideration, provides the Government with the authority to compel a company to share sensitive information over the company's legitimate concerns. This is particularly concerning to industry, particularly considering the Australian Signal Directorate's publicly acknowledged cyber offensive capability and the potential for compelled information to be used for this purpose.

Companies should not be compelled to share information with the Government that could put other customers around the world at risk. Companies need to be able to assess the risk of such sharing and make the decision on what data should be shared and under what conditions. The act of compelling access to information should be used by the Government only in extreme situations and with sufficient checks and balances in place to prevent the misuse of shared information.

BSA recommends that all shared information under this scheme relating to the CI operator should be treated as highly sensitive data and explicitly exempt from FOI 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 only be attributable with the permission of the sharing organisation.

System information software

The Bill proposes to give the Government the power to compel the installation of software on CI operator systems, potentially against the wishes and advice of the system operator.

BSA strongly objects to this proposal. Introducing any software or new capability into enterprise IT systems should only be done following a rigorous change management process to mitigate the risk to the security and stability of company systems. As proposed under the Bill, software could 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 company systems can compromise users' confidence in the integrity and trustworthiness of the company's products and services, undermining the business's competitiveness.

This is particularly critical for CSPs, where installing untested and thus potentially unsuitable software on global infrastructure puts huge investments at risk.

BSA recommends that the Bill provide the Government with the right to request but not the authority to compel the installation of software on CI operator systems.

Step-in powers

The Government is proposing to reserve a wide range of "step-in" powers in the event of a critical or catastrophic cyber event. While BSA supports the Government's desire to have the ability to help protect Australian interests should the worst occur, the Government has not made a clear case that the current state of affairs is ineffective or impracticable, particularly in the case of CSPs. If these powers are indeed necessary, they should be designed in such a way that builds trust in the intervention mechanism by ensuring sufficient oversight and due process.

Under the proposed powers, the Government reserves the right to step-in should a company be adjudged to be "'unwilling" or "unable" to comply with a request. There may be legitimate reasons why a company may be unwilling or unable to comply with a Government request. This is particularly relevant to CSPs where, under a shared responsibility model, the CSP may not be responsible for,

nor technically capable of, accessing data or otherwise responding to the Government's request. Under these circumstances, it is more appropriate for the Government to mitigate the incident via the CSP customer (i.e. the CI operator) than through the CSP itself.

Alternatively, a CSP, being the entity with the best understanding of the technical aspects of its system, may be unwilling to undertake an action because it would not mitigate the incident and may in fact make it worse.

Compelling action from a CSP under these scenarios distracts from addressing the incident and can interfere with efforts to mitigate the situation. BSA recommends the Government narrow its ability to forcefully intervene to specific cases, such as where CI operators are prevented from acting due to contractual issues, and add appropriate oversight and due process mechanisms to these powers.

Conclusion

The issues concerning the protection of critical infrastructure in Australia are vital to the security and resilience of the Australian economy. BSA and our members remain at the disposal of the Committee to help develop and deliver other enduring solutions to address the security of critical infrastructure. If you require any clarification or further information in respect of this submission, please contact the undersigned at brianf@bsa.org or +65 8328 0140.

Yours faithfully,

Brian Fletcher

Director, Policy – APAC

BSA | The Software Alliance