27 Nov 2020

Department of Home Affairs

Submitted Electronically

CRITICAL INFRASTRUCTURE BILL — BSA COMMENTS

BSA | The Software Alliance (**BSA**) appreciates the opportunity to provide comments to the Australian Government on the proposed Critical Infrastructure Bill[1] (the **Bill**).

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA's members[2] are among the world's most innovative companies, creating software solutions that spark the economy. BSA 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 fully supports the Government's efforts to update its framework to protect infrastructure that is critical for the functioning of Australia. As Australian critical infrastructure (**CI**) operators largely reside in the private sector, as in most countries, we are grateful to see that the approach to developing such a framework promotes close public-private collaboration and attempts to reflect the needs and objectives of all stakeholders.

However, BSA remains concerned with many of the expanded powers the draft Bill would grant to the Australian Government, and again cautions against the speed by which the Government is attempting to give itself these broad and extensive powers over a large portion of the Australian economy. The time provided for consultation on this draft legislation is not sufficient for meaningful engagement with all stakeholders, including cloud services and information technology providers, such as BSA members.

[1] Protecting Critical Infrastructure and Systems of national Significance, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

[2] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, 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.

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

This document is BSA's response to the draft Bill and the associated *Security Legislation Amendment (Critical Infrastructure) Bill 2020: Explanatory Document*[3] (the **Document**).

BSA and Critical Infrastructure Protection

BSA responded[4] to the *Protecting Critical Infrastructure and Systems of National Significance* consultation paper released in September 2020. In that submission, we described the broad principles that should inform CI security policies. Those being that CI security policies should be risk-based and prioritized, technology neutral, practicable, flexible, and respectful of privacy and due process.

Many of BSA's concerns from that initial consultation have not been addressed and remain in the proposed Bill. These include:

- Inclusion of new CI sectors — the broad nature of the proposed CI definition threatens to overwhelm operators of important, but not critical, infrastructure with obligations best reserved for those involved in supporting truly essential systems. Overly broad definitions such as these also create regulatory requirements that cause limited government resources to be spread too thin to be effective.[5]

- Proposed new data storage or processing sector — the proposed "data storage and processing" sector is quite different in nature from the other proposed CI 'industry vertical' sectors proposed in the discussion paper. "Data storage and processing" is not an industry in itself, but instead represents companies, technologies, and services that cut across the entire economy, serving a broad swathe of industry verticals. Designating "data storage and processing" as CI in its own right will lead to businesses providing such technologies and services being held to multiple overlapping Australian regulatory requirements including the Government's Information Security Registered Assessors Program (**IRAP**) certification.[6]

- Positive security obligations — the proposed compliance-based scheme risks diverting valuable CI operator resources towards compliance processes and away from understanding and mitigating risks to their businesses.[7]

- Lack of due process for step-in powers — the Bill grants many new "step-in" powers to the Government. Although CI operators are required to be consulted, the Bill does not appear to provide sufficient due process or establish any rights of appeal regarding decisions of the Government for the affected companies.[8]

- Use of internationally recognized standards — regulations, policies, and standards issued by a government to address CI cybersecurity should be aligned with internationally recognized technical standards and internationally recognized approaches to risk management to reduce unnecessary and counter-productive regulatory burden.[9]

---

[3] Protecting Critical Infrastructure and Systems of National Significance, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

[4] BSA Response to Critical Infrastructure Consultation Paper, https://www.bsa.org/policy-filings/australia-bsa-response-to-critical-infrastructure-consultation-paper

[5] Ibid., p3

[6] Ibid., pp 3-4

[7] Ibid., pp5-6

[8] Ibid., p6

[9] Ibid., pp6-7

Recommendations

In summary, we recommend that the Government amend the Bill to:

- Eliminate the proposed designation of "Data Storage and Processing Sector" as CI.
- Narrow the definition of what is considered CI and "business critical data".
- Establish a voluntary public-private partnership model with adequate incentives to drive participation by the relevant private sector stakeholders and refrain from compelling participation in such a partnership.
- Establish a risk-based incident reporting mechanism that recognizes the first priorities of CI providers and their partners are to identify, diagnose, and mitigate an incident, and then to provide notification to their customers and/or the Government.
- Recognize that cloud service providers (**CSPs**) and other data storage and processing providers, under the "shared responsibility" model, may not know or be able to respond to particular Government requests or requirements, and ensure that obligations are imposed on CSP customers, including CI operators, instead.
- Avoid undermining physical security by requiring the disclosure of data center locations.
- Ensure any data that is shared with the Government by CI operators and their commercial partners, whether voluntarily or under compulsion, is strictly protected against misuse or disclosure, including against Freedom of Information (**FOI**) requests.
- Eliminate any requirements to install government software in CI operators' IT systems or the systems of their IT providers.
- Minimize Government "step-in" powers to ensure that company concerns are taken into consideration and they are not imposed on global CSPs when they should be imposed on the CI operators.

DETAILS

Proposed Data Storage or Processing Sector

The definition for the "Data Storage or Processing Sector" is currently extremely broad. There are two main requirements proposed in the Bill for an asset to be considered "critical". The first requirement is whether the asset is being knowingly provided to the Commonwealth, or a State or Territory Government, or any body corporate in Australia.

This is overly broad. Within organisations, not all assets, systems, networks, data, and services are equally essential. It is important that CI policies 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. Accordingly, the first requirement in this definition should similarly be limited to assets providing critical services and functions, and whose compromise, damage, or destruction through a serious cybersecurity incident could result in significant economic or physical harm to the public.[10]

The second requirement is whether the asset knowingly handles any "business critical data" for other CI assets. The Bill defines business critical data, among other considerations, including 20,000 or more personal data records, or any amount of sensitive personal data as defined under the *Privacy*

[10] BSA International Cybersecurity Framework, https://www.bsa.org/reports/bsa-international-cybersecurity-framework

Act 1988. The Privacy Act Review discussion paper released by the Attorney-General's Department (**AGD**) notes unclear under the current definition of personal information what types of technical data is considered to be personal information under the Privacy Act, and recommends this being clarified.[11] If the AGD applies a broad inclusion of technical data to the definition of personal information (e.g. to include common technical data such as IP addresses and email addresses), the definition would encompass even more entitites than anticipated — increasing the scope of business critical data and broadening the definition of the proposed sector even further.

We remain concerned that, unlike all the other proposed "vertically aligned" sectors, the proposed data storage and processing sector is a horizontal sector that provides services to all other sectors of the economy. By designating data storage and processing providers as CI, CSPs and others will be subject to the cybersecurity requirements of all 15 critical infrastructure sectors' regulators, in addition to the Department of Home Affairs (**DHA**) as the regulator for the data storage and processing sector. Those enterprises that provide services to government customers will additionally need to follow the Government's IRAP requirements. This is a very inefficient approach to security that will increase costs of operation and reduce productivity without increasing security outcomes for Australia.

In sum, BSA recommends that the Government amend the Bill to remove the definition of the data storage and processing sector as a CI sector, and instead make it clear that data storage and processing providers will need to follow the requirements of their Australian CI customers, if and when they provide relevant technologies and services to them.

Partnership with Industry

At several points in the Document, the Government expresses the desire to partner with industry on the protection of CI in Australia. BSA applauds this approach and is a strong proponent of government and industry working together to solve issues such as these. There are many different public-private-partnership models. 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 data storage and processing providers, among others. Such partnerships aim to reduce costs and risk while achieving the goals of the government by leveraging the capabilities of the private sector, they are built on trust and mutual benefit.

In some cases, governments have established clearly structured partnerships with relevant private sector stakeholders to share cybersecurity information. In such cases, laws should protect providers sharing information from liability and anti-trust concerns and enable bi-directional sharing of information between the public and private sectors. In such cases, providers benefit from receiving timely threat information from the government, which enables them to improve their network defenses, while the government is able to obtain threat information from businesses across a wide range of sectors and threat environments. Such partnerships work because they are voluntary, mutually beneficial, and clearly structured.

Instead, 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 and two-way information sharing, for private sector participation by the relevant private sector stakeholders.

Positive Security Obligation

Critical cyber incident reporting

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

[11] Privacy Act Review Issues Paper, https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf, p18

availability of the asset or a critical impact on the operation of critical infrastructure entities within Australia.

The threshold for reporting a cybersecurity incident included in the Bill is inappropriately broad. The trigger for reporting should be strongly tied to a material and serious impact to CI under the definition of the sector, with incidents occurring outside of the context of CI (as defined in section 12F), explicitly not subject to the reporting requirement.

The reporting threshold in the Bill for this requirement is extremely low. There does not seem to be a definition for significant impact, but the definition of "relevant impact" (section 8G) referenced under this requirement has no minimum threshold. Events under the definition of relevant impact require CI operators to provide a written report. Considering there is no minimum threshold, this is an unacceptable burden on CI operators.

In the event of a truly significant incident, the attention and resources of a CI operator, and that of their storage or processing providers, should be focused on diagnosing and remediating the incident, and notifying the impacted customer if appropriate. Extremely short 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.

Furthermore, 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 the incident reporting requirement should have a risk-based significant impact test, encompassing either scale or impact on CI entities in Australia. The scheme should allow for events that occur at a lower threshold to be reported voluntarily via a low impact process.

BSA additionally recommends amending the incident reporting requirements so that providers notify the 'fact of' a reportable incident and following up with written reporting 'as soon as possible', allowing time for incident investigation in line with provisions under the notifiable data breaches scheme (Privacy Act 1988).

Ownership reporting obligation

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

The location of data centers 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 ever force providers to share. Asset owners should have the opportunity to voluntarily provide this information after conducting an assessment of the risk to the asset. Furthermore, this information should be exempt from FOI and other information requests.

Sector specific rules

The success of the Bill will depend, in part, on how the co-design process for sector specific rules will work and be maintained into the future. How these rules will be decided, and the details of implementation, are essential considerations for industry when commenting on the Bill. DHA noted in the "'Town Hall" attended by BSA on 12 November 2020, that work on the sector specific rules cannot start until the legislation is enacted.

BSA recommends that the Government outline these details as soon as possible to help deliberations on the Bill. In particular, the Government should include considerations such as:

- What role will industry have in the co-design process for establishing sector specific rules and how will disagreements be settled, particularly between industry and government?

- How will the Government ensure that all sector members are treated fairly and not subject to unfair, anticompetitive actions by other sector members?

These considerations will be increasingly important in sectors in which the Government has little experience or expertise, such as in operating large scale data storage or processing operations. BSA is particularly concerned about ensuring due process is observed as sector specific rules are developed and applied. A co-design process is more than an extended consultation process and is not one where the Government has the final say against the concerns of industry attendees.

Every effort should be made to keep sector specific rules risk based. CI sectors are often diverse in terms of technological infrastructure, involve different types of risk, and confront different threats and threat actors. More importantly, the technology used in these infrastructures are diverse and constantly evolving. Overly directive or prescriptive regulation 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.

Sector specific rules should focus security policies on driving desired security outcomes, providing private sector entities latitude to develop the most effective, 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 decision about cybersecurity resource allocation to align defenses against the most pressing risks.

The ability to turn some obligations on and off via Ministerial Authorisation is a useful feature of the Bill. However, BSA is concerned that rules may be unevenly applied, providing an unfair competitive advantage to some operators, for example if it was used to provide a lower regulatory requirement for some entities than others.

Furthermore, the Government should not impose rules that encourage CI operators to establish their own data centers simply to avoid compliance with rules applied to commercial data storage and processing entities. This would result in a less secure and capable cloud computing environment for CI operators.

Enhanced security obligations

Sharing "system information"

As part of the initial consultation, the Document notes several times that many responders, including BSA, observed the need for more information shared by the Government on potential threats. Despite the request for more information from the Government, the Document instead suggests compelling companies to release sensitive data to the Government. The quickest and most effective way for the Government to support CI operators would be to automatically share all relevant threat information in government holdings with them early and without restriction.

Compelling system data from CI operators both misses the point of requests for further information, and the power of a voluntary data sharing program. To be useful to the CI community and to encourage further collaboration between the private sector and the Government, information sharing must be multidirectional. Governments should share all existing relevant cybersecurity threat information with private parties, particularly those deemed to be CI, and do so in a timely manner.

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, CI operators should not be held liable for choosing not to share information with other private entities or governments outside of commercial vendor-customer relationships.

Furthermore, information sharing with Government should be strictly limited to data that relates to the "critical asset" being serviced by the provider and should only be shared with the full knowledge and concurrence of the customer that operates the asset.

The Government should take steps to reduce the risk to CI operators from loss of control and misuse of the information shared. If CI operators are compelled to share such system information as proposed, the data will be very sensitive to the company and, if lost or uncontrolled, could allow malicious cyber actors to cause them significant damage. Such data should be protected to an extremely high level. All shared information under this scheme should be exempt from FOI requests and other data release schemes.

Information sharing policies should ensure shared cybersecurity threat information is used by the recipient only to promote cybersecurity and for no other purpose. When sensitive information is shared with governments, the information should be used only to promote cybersecurity or for limited law enforcement activities against malicious cyber actors, and should only be attributable with the permission of the sharing organisation.

This is particularly important considering ASD's publicly acknowledged cyber offensive capability. 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 information should only be used in extreme situations, and with checks and balances in place to prevent the misuse of shared information. The Bill, except for a vague requirement to take a company's views into consideration, seems to provide the Government with the authority to compel a company to share sensitive information over the company's legitimate concerns.

Finally, BSA is concerned that these information sharing requirements are in addition to existing, successful private sector sharing activities. Compelling CI operators to share information with the Government could put the sustainability of the existing sharing activities at risk as some members of the CI community would be forced to prioritise sharing with the Government over potentially more useful mechanisms.

System information software

BSA strongly objects to the Government granting themselves the power to compel the installation of software on CI operator systems. Such a requirement would introduce a high amount of risk to the security and stability of company systems without adequate testing or vetting by company staff who understand the operation of the data storage or processing asset and the interdependencies of the entire system. Moreover, mandatory installation of government software on company systems can compromise users' trust in the integrity and trustworthiness of the company's products and services, undermining the business's competitiveness.

This is particularly critical in for data storage and processing providers, where installing untested and thus potentially unsuitable software on global infrastructure puts huge investments at risk. Nothing should ever be installed on company systems without the full knowledge and concurrence of the CI operator.

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 for providers of data storage or processing products. If these powers are indeed necessary, they should be done in such a way that builds trust in the process with sufficient oversight and due process.

Under these 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 cloud services 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. 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. The Government should instead narrow its ability to forcefully intervene to specific cases such as where CI operators are prevented from acting due to contractual issues. This can be done by building structures to better collaborate with CI operators and provide mechanisms for an operator to request Government intervention if needed.

Conclusion

Securing CI will be an ongoing challenge — one in which security techniques must adapt to an ever-changing environment of new technologies and new threats. BSA commends the Government for this contribution to CI protection in Australia.

BSA thanks the Australian Government for providing the opportunity to comment on the Bill and we look forward to continuing to collaborate with the Government on CI protection policies. 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