16 September 2020

Department of Home Affairs

ci.reforms@homeaffairs.gov.au

Submitted electronically

BSA RESPONSE TO CRITICAL INFRASTRUCTURE CONSULTATION PAPER

BSA | The Software Alliance is grateful for this opportunity to make a submission to the Department of Home Affairs on the Critical Infrastructure Centre's discussion paper, *Protecting Critical Infrastructure and Systems of National Significance*.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members[1] are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. BSA members have made significant investments in Australia and are proud that many Australian organisations and consumers continue to rely on BSA member products and services to support Australia's economy.

Initial comments

BSA fully supports the Australian Government's move 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.

We note that there are still many details to be worked out, including some very fundamental questions about the scope of critical infrastructure and what protective measures are proposed. As such, industry needs time to understand where they may fit into the proposed framework, the impact on operations and what regulator to work with. Given the importance and potential impact of these changes, BSA is concerned that the Government has not allocated sufficient time to fully consult on these changes. We respectfully recommend that the Australian Government provide adequate opportunities for further consultation as the legislation and associated policies are considered, particularly on whether and how to address cloud computing and data-related services under this proposal.

[1] BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, 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

Principles for Critical Infrastructure Security

Technology evolves rapidly and in unpredictable new directions. It is thus essential that any policy framework for critical infrastructure cybersecurity use security measures that are sufficiently agile and adaptable to avoid stifling innovation and economic development. Prescriptive regulation is ill-suited to address fast-paced cyber threats and malicious actors that find new ways to launch attacks. Onerous reporting and compliance mandates, such as those relating to the contemplated audits, risk assessments, and incident reporting force businesses to divert scarce resources away from proactively managing evolving cyber risks to fulfilling requirements that quickly become outdated.

To achieve balance between security, adaptability, and innovation, a critical infrastructure cybersecurity framework should be based on the following key principles:[2]

1. **Risk-Based and Prioritized.** Cybersecurity threats come in many forms and magnitudes with varying degrees of severity. Establishing a hierarchy of priorities — based on an objective assessment of risk[3] — with critical assets and/or critical sectors at the top is an effective starting point from which to ensure that cyber protections are focused on those areas where the potential for harm is greatest.

2. **Technology-Neutral.** CI operators should be empowered to use the best security technologies. A technology-neutral approach to cybersecurity protection is vital to ensure access to the most secure and effective solutions in the marketplace. Specific requirements or policies that mandate or prohibit the use of certain technology only undermine security by restricting evolving security controls[4] and best practices and potentially creating single points of failure.

3. **Practicable.** Overly burdensome government supervision of private operators or disproportionately intrusive regulatory intervention in their operational management of cybersecurity risk most often proves counterproductive, diverting resources from effective and scalable protection to fragmented administrative compliance. Instead, a framework should establish standards and security measures that are accessible and scalable across the range of covered entities.

4. **Flexible.** Managing cyber risk is a cross-disciplinary function and no one-size-fits-all approach exists. Each industry, system, and business faces distinct challenges, and the range of responsible actors must have flexibility to address their unique needs.

5. **Respectful of Privacy and Due Process.** Security requirements should be oriented to protect privacy and due process. Ensuring that requirements and obligations are proportionate, do not unnecessarily intrude upon privacy rights, follow due process, and are supported by adequate judicial oversight are all important considerations to address in any CI cybersecurity framework

---

[2] BSA Cybersecurity Policy Framework, https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf, pp13-14

[3] Risk can be defined as "an expression of the effect of uncertainty on cybersecurity objectives, as understood through the analysis of identified threats to a product or system, the known vulnerabilities of that product or system, and the potential consequences of the compromise of the product or service. Ibid., p24

[4] A security control may be defined as a "management, operational, or technical control used to protect against unauthorized efforts to adversely affect the confidentiality, integrity, and availability of an information system or its information." Ibid., p24

These principles should be rooted in public-private collaboration. Cybersecurity is a shared responsibility across government and private stakeholders. Although governments often hold critical cybersecurity tools and information, the private sector is responsible for significant elements of CI and the technology platforms that are targeted by malicious cyber activity, as well as many of the cybersecurity tools and services necessary to defend against such threats. Only by working in close collaboration with the private sector can governments truly combat cybersecurity threats while sustaining the vitality of the digital economy.

Governments around the world are struggling with the same questions for the security of their own CI sectors. They are facing many of the same risks and looking to use the same defensive approaches and technologies as the Australian Government. Any approach the Australian Government takes in this space should be internationally interoperable and based on internationally recognized standards and should have provisions for reciprocity where possible.

What entities will be covered? (Questions 1-6)

Q1 Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms?

BSA recommends that countries avoid applying overbroad definitions of CI. Broad definitions cause uncertainty among business owners, their providers, and government agencies for compliance and during enforcement. Such definitions are likely to create costly regulatory burdens, reducing productivity without improving cybersecurity, and throttling innovation in an economy. Such an approach ends up overwhelming operators of important, but not critical, infrastructure with obligations best reserved for those involved in supporting truly essential systems. It can also create requirements that cause limited government resources to be spread too thin to be effective.

While many sectors can be considered important to a country, not all can nor should be considered critical. We recommend that governments to apply a rigorous, proportionate, and risk-based analysis to determine what infrastructure should be designated as truly critical.

Overly broad definitions can also lead to overwhelming regulatory authorities with unnecessary information and with oversight and enforcement responsibilities that do little to increase security. There are numerous examples from around the world where overly broad approaches have led to regulatory failure. An example of this is the now defunct Australian Cyber Security Centre's (ACSC) Certified Cloud Security List.

Data and the Cloud as a sector

BSA is concerned with the proposal to establish a horizontal 'Data and the Cloud' (**DatC**) CI sector to cover data centers and cloud service providers (**CSP**s). The suggested sector is quite different in nature from the other 'industry vertical' sectors proposed in the discussion paper in that it is not an industry in itself, but instead cuts across the entire economy serving a broad swathe of industry verticals.

It is also unclear what problem the Australian Government is trying to solve by establishing the DatC CI sector or why existing approaches to collaboration in this space are considered not sufficient.

BSA is corned that establishing a DatC CI sector creates a real threat of over regulation. CSPs in the proposed DatC CI sector already meet sectoral obligations and the separate obligations of all their customers, some of whom could likewise be CI operators with their own sectoral obligations and regulators. Many CSPs also serve Australian Government customers and have separate government security obligations to meet for them. Imposing duplicated and overlapping requirements on such

service providers could add considerable overhead to operations and slow the release of new and innovative products for all Australian customers.

It is currently unclear whether a CSP designated as part of the proposed DatC CI sector would then need to apply the respective CI sectoral obligations to all customers in Australia, whether CI obligations are limited to a subset of products, or whether CI obligations only apply to products and services provided to 'designated' customers. If CSPs designated as DatC providers have broad additional obligations imposed upon them, such CI operators could be placed at a substantial disadvantage to other CSPs that do not have to comply with such requirements, skewing the CSP marketplace in Australia.

Furthermore, 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 a customer and their CSP. This "shared responsibility" security model is a very important principle of cloud security. Imposing security controls and reporting obligations on the CSP alone could undermine the existing security arrangement between CSP and their customer. For example, the regulations could apply security obligations on the CSP regarding activities that are the responsibility of the customer, and therefore outside of the CSP's visibility and control. In addition, the reporting obligation for a potential incident should lie with the customer, as the affected organisation. Should a potential incident be detected by a CSP, their first obligation should be reporting to the customer for further investigation before it can be determined if it is a security incident.

From a regulatory perspective, Australia should not be creating a DatC CI sector. Instead the Australian Government should require that CI operators from other 'vertical' CI sectors ensure any CSP they use can comply with their specific CI sector requirements. This gives CI operators the ability to choose CSPs or other solution providers consistent with their security requirements; a CI approach that recognizes this flexibility and sets expectations for CI operators to make responsible choices to securely manage data and Internet requirements addresses important CI security considerations without creating a burdensome horizontal structure that quickly stretches beyond the bounds of CI.

Q4 What are the common threats you routinely prepare for and those you have faced/experienced as a business?

BSA members operate global software and cloud businesses serving a wide range of customers and holding a wide array of important data. As such, they invest heavily in security programs and have experience at successfully dealing with the full spectrum of threats including government-based groups, criminal gangs, and issue-motivated groups.

Among the risks that BSA members commonly address is secure software and vulnerabilities. CI operators can use tools like the BSA Framework for Secure Software[5] to assess the security of the software and cloud services they purchase. In addition, as CI operators prepare their own code and software continues to evolve, operators should consider operating a coordinated vulnerability disclosure program.[6]

Q5 How should criticality be assessed to ensure the most important entities are covered by the framework?

Criticality should be determined by a robust and open risk management process, undertaken in conjunction with the sector. It should take an all-threats approach to the assessment.

[5] https://www.bsa.org/reports/bsa-framework-for-secure-software

[6] https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdf

Q6 Which entities would you expect to be owners and operators of 'systems of national significance'?

Collaboration (Questions 7-9)

Many of the questions from this section relate to the Trusted Information Sharing Network (TISN). It is not possible for BSA to comment on the TISN without first having been a member as public details on the program and how it operates are limited.

As proposed, it is plausible that the Government would seek share CI operators' commercially sensitive information with competitors in the sector under this scheme. It is unclear how the Government intends to avoid this commercially risky situation or protect against damages arising from such sharing.

We also note that there are numerous existing voluntary industry-led security data sharing arrangements already in place that have been very successful in providing protection to several entities that would fall under these new rules. The Government should be careful to not disrupt these existing successful industry-led initiatives.

Q9 How else should government support critical infrastructure entities to effectively understand and manage risks?

In general, government sharing schemes around the world have been marred by over classification of data, limited usefulness of data, exclusion of entities, and poor sharing mechanisms with industry. Government sharing of threat data with CI operators is most useful when done without restriction, notifying CI operators of all malicious activity known to the Government.

Noting that the Government intends to apply an all-hazards approach, data sharing from the public sector in return should reflect this and not be limited to just cybersecurity.

Positive Security Obligation I (Questions 10-14)

CI sectors are often diverse in terms of technological infrastructure, involve different types of risk, and confront different threats and threat actors. Moreover, the technologies used in these infrastructures are diverse and constantly evolving. Overly directive regulation focusing on specific methods or strict compliance, or mandates that limit the use of security enhancing technologies such as encryption can cause further issues for CI operators. Rather than improving security, they can bog down adaptive security measures and stifle innovation across the private sector.

Instead, governments should focus CI cybersecurity policies on driving desired security outcomes, increasing operators' visibility of threats, 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 organizations to prioritize cybersecurity activities and make informed decisions about cybersecurity resource allocation to align defenses against the most pressing risks.

As currently described, the proposed CI regime, although containing aspects of a risk management approach, is a compliance scheme in which regulators determine if "proposed mitigations are proportionate to the risks."[7]

A compliance-based scheme risks diverting valuable CI operator resources towards compliance processes and away from understanding and mitigating risks. This is particularly important as CI operators under the scheme seem to maintain responsibility and liability for their infrastructure in the

[7] P18 of the consultation paper; also notes that operators are to mitigate risks to 'prevent incidents'

event of incidents. They cannot do this if the Government is taking responsibility for risk assessment on their behalf or forcing potentially ineffective compliance requirements on them.

An example of this is the requirement for CI operators to submit their risk assessments for Government approval. Risk assessment documents are important internal documents used for the documenting the threat environment, noting risks and their corresponding compensating mitigation controls and, ultimately understanding the residual risk. They are for security teams to communicate with operational colleagues and as a communication device with senior management for acceptance.

Risk assessments are not compliance documents. BSA is concerned that using them as such will subvert their usefulness to the organization, decrease the effectiveness of their risk management practices, and ultimately, risk of exposing sensitive vulnerability data beyond the 'need to know' basis.

BSA notes that, the process lacks the ability to allow companies to disagree with regulator assessments of risk and 'compliance'. This is particularly important if the regulator requires changes in the CI operator's system that in the perspective of the operator puts other customers at risk, causes damage to critical systems, would be ineffective in the view of the CI operator, or mandates excessively elaborate or expensive controls that are better achieved through alternate means. This could represent an open-ended risk to CSPs' security and ongoing operations.

BSA recommends that the Australian Government looks to adopt an existing cybersecurity certification scheme based on a risk-based framework.

Q11 Do you think the security obligations strike the best balance between providing clear expectations and the ability to customize for sectoral needs?

BSA fully supports the Australian Government's desire to introduce principle-based security obligations for physical, cyber, personnel and supply chain security of CI operators. This flexible, outcome-focused approach is exactly what will achieve long-term robust security compliance in critical infrastructure. The application of these principles should similarly be principle-based and rooted in a risk management approach when applied by individual sector regulators.

The Government should ensure that requirements follow internationally recognized standards and should not apply requirements to disclose source code and other related intellectual property.

Standards

Standards and best practices are most effective when developed in collaboration with the private sector, adopted on a voluntary basis, and recognized globally. 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, such as the ISO/IEC 27000 and ISO/IEC 62443 series of information security management standards, the Common Criteria for Information Technology Security Evaluation, or the US Government's NIST Framework for Improving Critical Infrastructure Cybersecurity, as appropriate.

Governments should particularly emphasize alignment with those standards developed through voluntary, consensus-based processes. Allowing CI operators to combat evolving cybersecurity threats with evolving best practices and standards permits a more flexible, current, and risk-based approach to cybersecurity. Moreover, use of internationally recognized standards ensures interoperability for both businesses and government agencies with international counterparts, facilitating both economic development and operational collaboration against cybersecurity threats.

Some governments are imposing country-specific standards for CI cybersecurity, arguing that it will lead to improved cybersecurity. The real effect, however, is the opposite. Government-imposed indigenous standards inconsistent with globally accepted best practices and standards, rather than bolstering security, tend to freeze innovation and force consumers and businesses into using products that might not suit their needs. Such an approach can prevent CI operators from integrating security technologies that represent best-in-class solutions.

Certification[8] regimes may be effective measures to drive stronger cybersecurity in the CI community. To do so they must be strongly rooted in risk management principles and not used to enforce compliance approaches to security, They should also structured in a way that both promotes security needs and addresses market demands for both continuing innovation and broad diversity of product types and configurations.

Source Code and Other Intellectual Property

Some countries have imposed laws requiring developers of certain products to make source code and related intellectual property available for inspection before such products can be used in critical infrastructure. Such requirements are inappropriate and ineffectual. Requirements to disclose source code, enterprise standards, security testing results, and similar proprietary information pose significant inherent risks to intellectual property protection, while providing little added security value.

Because many of today's technology products include millions of lines of code, inspectors simply are not capable of reliably identifying single code flaws. If governments lose control of code disclosed by software developers, it be used by an attacker to discover and refine attack methods. Governments should avoid any law requiring the transfer of, or access to, source code of as a condition for the import, distribution, sale or use of such software or products.

Q12 Are organisations you are familiar with already doing this?

BSA members operate an enormous amount of IT infrastructure across the world. They invest heavily in certifications against international security standards and are world leaders in this space.

There is a concern that Government operated networks, which themselves are critical to the nation, are not following these policies, as evidenced by problematic Australian National Audit Office cybersecurity audit reports. This could make them a weak spot in a larger view of critical systems in Australia and should be given the same amount of scrutiny and support.

Q13 What costs would organisations take on to meet these new obligations?

BSA believes that if these obligations are based on international standards, they are not new requirements and are the cost of doing business for responsible companies in this space. If the Australian Government chooses to use an indigenous standard, it is impossible to estimate the costs as it depends on specific indigenous security requirements. Even for companies compliant with international standards, the cost of meeting unique indigenous requirements could be significant.

In both cases, the cost of uplift for companies without a current healthy security culture could be considerable and could require a major rearchitecting of their business.

Positive Security Obligation II – Regulators (Questions 15-21)

The Australian Government proposes to appoint a regulator to each of the proposed CI sectors to monitor compliance with the positive security obligation and enforcing these obligations. Their role

[8] Certification may be defined as 'third-part attestation (IE issue of a statement) that specified requirements related to products, processes, systems or persons have been fulfilled. BSA Cybersecurity Policy Framework, https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf; p22

seems to be to develop voluntary guidance, ensure CI operators comply with them, issue security notices and penalizing CI operators for non-compliance[9].

These regulators will handle both highly sensitive security information, and very sensitive commercial information and will be the target for malicious actors. Loss of control of operators' information could both be a serious concern to the security of the sector and be financially devastating to operators. In addition, by providing Government access to sensitive information, the security of customers in other jurisdictions could be perceived to be put at risk, and thus limit operator's ability to operate overseas.

It is also not clear which regulator would take the lead in event of a disagreement between regulators on CSP security controls or incidents. Disagreements involving the DatC regulator and potentially multiple customer regulators could leave CSPs stuck in a position of having to comply with conflicting requirements from multiple regulators. The Australian Government should consider a mechanism for easily deconflicting between disagreeing regulators or to coordinate in the event of a large-scale, cross-sectoral incidents. An example is the 'single point of contact' provision recently created in the EU.

Penalties

The Australian Government should be cautious about introducing a penalty regime for CI operators under this scheme. Whilst BSA supports such a scheme whereby regulatory agencies can provide specific directions to CI owners with fines or injunctive relief to sanction non-compliance, such a scheme should incentivize the right outcomes.

We further urge the Government to ensure that there are appropriate checks and balances in place to ensure CI operators are able to appeal in instances where they disagree with a regulator's assessment or demand, and to guard against the abuse of these powers.

Q15 Would the proposed regulatory model avoid duplication with existing oversight requirements?

As noted earlier, BSA is highly concerned about the duplicative nature of the proposed scheme with regards to a proposed DatC sector.

Q17 Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related role? What might be the limitations to that organisation taking on the role?

The resourcing, skills and staffing to regulate a DatC sector would be unique in the world. There is no Government body in Australia capable of regulating the cloud service sector, although the Australian Signals Directorate (ASD), with their Information Security authority would come closest. BSA notes that ASD should only be made the regulator if they are willing and able to resource the mission appropriately to avoid a similar programmatic failure as occurred with the Certified Cloud Security List.

However, BSA also notes that giving ASD the role would give them access to sensitive company information that could put other customers around the world at risk and impact company's ability to operate in other jurisdictions. There may be concerns in other jurisdictions that there is insufficient separation between the information security aspects of the ASD mission and the other offensive activities they carry out.

[9] P22 of the discussion paper

Q19 How can government better support CI?

The Government can be support CI operators by sharing all relevant threat information with them early, and without restriction.

Q20 What do we think of the AusCheck system?

As there is little public information available, BSA is not able to assess the efficacy or overhead involved in participating in the AusCheck system and whether it could continue to operate through such a large increase in load. Centralised personnel clearance programs are one way to reduce risk but are not the only effective control. They can have issues with poor resourcing impacting throughput slowing recruitment and causing widespread personnel shortages.

Enhanced Cyber Security Obligation (Questions 22-28)

The scheme proposes creating a higher level of CI referred to as 'Systems of National Significance'. CI operators designated to this level would have to comply with enhanced cyber security obligations on top of the positive security obligations. These enhanced obligations consist of taking part in situational awareness and preparatory activities.

Noting that we do not know how the Government will determine participants, it is hard to comment on these aspects of the law.

Participation in preparatory activities

It is unclear what the Government is suggesting here making it difficult to comment, but it is assumed that the Government intends to carry out national event planning and incident exercises. These types of activities are very useful and BSA members participate in these in other jurisdictions. It is unclear how this obligation would be applied, whether they will be instructed to attend particular activities or if they will be offered a choice.

It is unclear what the Australian Government means by wanting to develop 'playbooks'. Playbooks are useful tools for personnel in Security Operating Centres that help deal with the many scenarios they face when dealing with various events. It is unclear how useful they would be in a wider context.

Q23 What information would you like to see shared with CI [operators] by Government? What benefits would you expect from greater sharing?

BSA is highly concerned about the situational awareness aspect of the scheme with there being obvious advantages to the Government and few for the CI Operators. Whilst it is initially proposed to be a voluntary scheme, the Government notes that it will become compulsory in time. At this stage, we do not know what information will be required to be shared, and whilst the discussion paper notes it should not contain customer data, it is likely to consist of highly sensitive security and commercial information.

Mandatory and broad threat and incident reporting requirements can be counterproductive. Frameworks that force companies to report cybersecurity incidents, leaving the thresholds for reporting broadly defined, can unintentionally inhibit cybersecurity by causing companies to over notify of any incident on their systems. It distracts security staff from reacting to the most important signals and can lead to notification fatigue, which makes it difficult to identify and address the most important incidents. As such, cyber threat or incident should be defined narrowly for reporting purposes.

As noted earlier, forcing companies to share such sensitive data represents a large security risk to CSPs. Governments should never force sensitive commercial information to be shared with them. Should the Government lose control of this data, it could represent huge commercial losses to the CSP. Information sharing arrangements are most successful when they are voluntary, build on trust,

enable bi-directional sharing, and they enable victims of attacks to share information about both successful intrusions and "near-miss" attempts without fear of being investigated as a result.

Governments that force sensitive commercial information to be shared with them should give unlimited liability to companies for losses due to government mishandling of the shared information.

A mandatory scheme would also be unlikely to move with the speed of technology. As technology changes, new data types will become relevant and available, with CSPs then locked into sharing nonsensical, or irrelevant information with the Government. They could be forced to run outdated, or unsafe equipment or configurations simply to provide outdated mandatory information requirements. This could put them in a situation whereby they are unable to take advantage of new innovations in security to provide the Australian Government and CI sector customers.

One aspect of situational awareness is Government sharing information with CSPs. BSA notes that members have received data from governments around the world, that whilst sometimes useful, if often irrelevant or outdated by time of sharing. One way to build trust with CSPs would be to offer that if threat info is known that could prevent an incident, and not shared, company should be reimbursed for the associated losses.

The Australian Government should share all relevant threat information with CI operators without restriction and in a timely manner. This might allow them to make better decisions on how to better protect their IT systems.

Q24 What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

BSA members already voluntarily share information with governments and customers around the world as part of routine business. Continuing that process, without change would have no cost implications.

Q25 What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

There is no one way to do this and it depends on the context. What is important, is that governments do not actively probe the networks of CI operators without the operators' full knowledge and concurrence. This is indistinguishable from malicious activity and distracts security staff from their job of protecting networks.

BSA notes that it is important for organisations to have and use vendors that have a coordinated vulnerability disclosure program[10]. Because vulnerabilities can be identified by external stakeholders, such as independent security researchers, it is critical for operators and their vendors to maintain procedures for processing such third-party reports of vulnerabilities on their networks.

Q26 What are the barriers to owners and operators acting on information alerts from government?

Generally, the industry is responsive to Government information alerts. However, information alerts from governments are often not timely, overclassified, and sometimes irrelevant.

[10] https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdf

Q27 What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with government?

The Government needs to articulate what outcomes they expect to achieve from the playbooks. As currently described, they would be of limited use to CSPs.

CI operators should not be forced to dedicate staff to an activity that will have no useful security outcome.

Q28 What safeguards or assurances would you expect to see for information provided to Government?

As noted earlier, there is a concern that the loss of sensitive CSP data could lead to large losses to their business. One way to build trust with CI operators would be to ensure that companies have an unlimited ability to claim for losses if data gained via mandatory disclosure requirements is lost by the Government.

Also as noted earlier, there may be concerns around the world about the ability for the Australian Government to force the release of commercially sensitive and security-based information and use it to compromise other customers around the world. The Government also needs to introduce a transparent and open system to prevent information gained by mandatory means from being used for the Government's offensive cyber program or to damage other customers.

BSA reiterates the assertion that mandatory acquired information should never include commercially sensitive information.

Cyber Assistance (Questions 29-36)

The third element of the Australian Government's plan is proposing to provide assistance to CI operators in the event of an incident. Transparency and public-private partnership are essential to successfully countering highly adaptive cybersecurity threats. It is not possible to develop effective governmental oversight for cybersecurity risk management without transparent policy development mechanisms.

Cyber incidents

The Australian Government has proposed that these powers are intended to only be used in-extremis. This is appropriate and the definition of cyber incident should be appropriately narrow to only encompass major events.

BSA notes that CI operators already operate in a world where they can request assistance from the government if needed, but a more formal framework could be useful.

Q29a In what extreme circumstances should [the] Government be able to take direct action in the national interest?

The Australian Government is proposing very strong powers in the event of an incident concerning a CI operator. These are powers that should only be used *in extremis*, and what is defined as an incident should be limited to encompass sufficiently serious events.

In the event of an incident, the Government should only act based on one of three triggers.

The first, and preferred manner would be on the request of the CI operator. If the incident is so extreme that the CI operator requires help, it should be able to call on the Government for assistance. For the Government to act without the concurrence of the company can distract staff from the important job of mitigating the incident, and risks making the situation worse, and further damaging critical company systems.

The second would be, if the CI operator is no longer able to make this decision, because it is not a functioning entity or if senior officers are no longer in charge or contactable. In this case, the decision to intervene would be made at a senior Government level (discussed below).

The third would be in the event of a large scale, multi-sector event. In this circumstance, individual companies are unlikely to be able to react on their own but should still be required to concur with any assistance offered.

Q29b What actions should be permissible.

All actions undertaken by the Government on CI operator networks should be with the full knowledge and concurrence of the operator, except in the example described above where the CI operator is not a functional entity.

Acts that would be illegal for the private sector to undertake should not be able to be performed on or with CI operator networks and assets.

Q30 Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

In normal circumstances, the company should be the only entity that is able to declare that a cyber incident requires Government assistance.

In the event that the company is not functioning or senior officers are non-contactable, or should there be a large scale, multi-sectoral event, either the Australian Attorney-General or the Prime Minister should be able to declare the circumstances requiring Government assistance.

Q32 If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

Where possible, law enforcement action should always be the first option for disrupting and holding accountable malicious cyber actors. Such perpetrators often operate outside the boundaries of the Government's jurisdiction, a fact which underscores the importance of international law enforcement cooperation in this area. Where law enforcement action is not possible, other disruptive options may be considered; in general, though, any Government action impacting a CI provider or other industry stakeholder should always be undertaken with the full knowledge and concurrence of that stakeholder.

Q33 What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

Individual industry and Government officers should be indemnified for their actions as long as they are acting legally, in good faith with the full knowledge and concurrence of the CI operator who owns and operates the networks being acted upon.

Industry personnel should not be asked to do anything illegal under any circumstance.

Government security teams work on the network of the CI operator could be problematic for a CSP. This may represent a security threat to personal and other commercially sensitive customer data that could risk future business for the CSP. Government operators would also be working in an environment they have little knowledge of, and experience on. If they conduct activities on the network without the full knowledge and concurrence of the company, the Government should be liable for any and all damages to company infrastructure or losses to operations if they were excessive or unnecessary to the immediate task of incident response.

Q34 What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type(s) of powers?

BSA recommends that governments should only gain access to or operate on industry-owned networks with the explicit permission of the network owner and all activities taken should be with the network owners' full knowledge and concurrence. However, in the event that Government compels access, operates on or instructs activities to be undertaken, companies should be afforded safe-harbour from any legal liability or regulatory consequences resulting from any Government access, instructions or activities on CI operators' networks..

As with any potentially risky Government powers, companies should have the access to judicial oversight of these powers.

BSA also believes that CI operators should be free to publicly communicate such access or compelled activities. They should be freely able to communicate publicly what happened under these provisions.

Q35 What are risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

There are many risks that these powers, if crafted poorly, could expose industry to.

- Companies could be excluded from other markets if Australian Government access to sensitive commercial information and forced access to networks are seen to potentially put other customers (including governments) at risk.

- Poorly conceived interventions by the Government could damage critical infrastructure and result in CI operators to repair.

- The cost of operating could increase for a large percentage of the Australian economy, increasing the cost of services and products for all Australians and Australian businesses

The Government should expressly indemnify CSPs from any subsequent legal cases or damages levied against them as a result of action taken by the Government on company networks that breaks any laws., They should also be able to retrieve the cost of any damage to infrastructure due to unnecessary or excessive Government actions on their networks..

Q36 Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

As currently prepared, the paper proposed an unbalanced regime that is based more on compliance than risk management principles. There is a high risk that CI operators are driven into a compliance-based approach to security that ultimately undermines the security of these important networks. It is also highly possible that mandatory actions imposed by the government to mitigate cybersecurity in isolation, undermines the stability and ability to operate of the CI systems themselves. The Government should instead focus on increasing the visibility of CI operators to the threat as they continue to maintain and operate their networks and provide technical support if required.

BSA supports the Australian Government's interest in ensuring the security of its CI. If done well, using risk management principles and in a voluntary fashion, this policy could have a large impact on increasing the cyber security of critical infrastructure in Australia.

It should also be noted that Government networks are themselves a vital part of the national cyber security picture. The Australian Government should make it a priority to uplift the cyber security of Government networks as both an exemplar and to demonstrate the commitment to cyber security of important networks in Australia.

We thank the Australian Government for engaging with industry on this important topic. Far reaching policies such as this take extensive consultation to be effective and BSA and its members remain committed to working with the Government. Cybersecure and resilient economies do not come about as a result of top-down legislation or regulation. Australia will continue to be a world leader in cybersecurity by promoting public-private collaboration, expanding trust-based information sharing exchanges, and supporting use of best-in-class cybersecurity solutions.

We appreciate your consideration of our concerns and look forward to working with you. 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