August 24, 2017

Via csa_cs_bill_feedback@csa.gov.sg

Dr. Yaacob Ibrahim
Minister
Ministry of Communications & Information
140 Hill Street #01-01A
Old Hill Street Police Station
Singapore 179369

Mr. David Koh
Chief Executive
Cyber Security Agency of Singapore
5 Maxwell Road #03-00 Tower Block
MND Complex
Singapore 069110

Subject: Public Consultation for the Cybersecurity Bill

Dear Dr. Yaacob and Mr. Koh:

The American Chamber of Commerce in Singapore (AmCham), BSA | The Software Alliance, the Coalition of Services Industries (CSI), the Information Technology Industry Council, the US-ASEAN Business Council, and the U.S. Chamber of Commerce express our gratitude to the Ministry of Communications & Information (MCI) and the Cyber Security Agency of Singapore (CSA) for the opportunity to submit comments on the draft Cybersecurity Bill (draft bill).

We congratulate you on being rated the top nation in the world for cybersecurity by a special agency of the United Nations. The draft bill is the next step in Singapore's cybersecurity journey. Achievements in this journey include: the passage of the Computer Misuse and Cybersecurity Act (1993) and its recent revision (2017); the establishment of the National Cyber Security Centre (2014); the establishment of the CSA (2015); the issuance of the Cybersecurity Strategy (2016) as well as numerous activities aimed at promoting cybersecurity in the region, and adopting the latest and most secure innovative technologies domestically.

The draft bill seeks to further strengthen Singapore's cybersecurity governance and legislative framework by laying out four objectives: (1) providing a framework for regulating critical information infrastructure (CII); (2) empowering CSA; (3) establishing a framework for sharing cybersecurity information; and (4) establishing a licensing framework for cybersecurity service providers.

While there are many aspects of the draft bill that are welcome and that are likely to further strengthen Singapore's cybersecurity, the members of our respective associations believe that changes to the draft bill are needed to best enable the legislation to meet the goal of improving cybersecurity in Singapore. We accordingly offer the following comments and recommendations:

- **Laws should avoid creating disincentives in the investment of security or slow its progress.** Policy and legal mechanisms can be put in place to support cybersecurity. For instance, legal avenues to permit fast sharing of threat information is critical, as well as laws promoting researchers to develop and test new security techniques. In this regard, bureaucratic paperwork-based strategy, licensing, and unilateral standards that go out of date quickly, would be a counterintuitive approach to fostering enhanced cybersecurity for Singapore. The draft bill should consider and also aim to promote security innovation. Policy frameworks that impose barriers for companies and individuals to enter the cybersecurity field work against Singapore's cybersecurity goals to level up cybersecurity and resilience.

- **Ensure that the definition and designation of critical information infrastructure (CII) are clear, appropriately limited, and consistent.** We agree with the core objective of the draft bill, which is to enhance cybersecurity and resilience for CII. However, broad definitions cause uncertainty for business owners, their providers, and the CSA during enforcement. We urge CSA to apply a rigorous, proportionate, and risk-based analysis to determine what should be designated CII. In addition, we would like to seek clarification that compliance with this draft bill is the responsibility of entities that provide essential services as defined in the First Schedule.

- **Codes of practices or standards of performance must leverage existing best practices and global industry-led standards.** Standards and best practices are most effective when developed in collaboration with the private sector, adopted on a voluntary basis, and recognized globally. Singapore should align any practices and standards it issues with industry-backed approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards or the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. Allowing CII operators to combat evolving cyber threats with evolving best practices and standards permits a more flexible, current, and risk-based approach to cybersecurity.

- **Prescriptive regulation is counterproductive.** Prescriptive regulation is ill-suited to address fast-paced cyber threats and malicious actors that find new ways to launch attacks on governments, companies, and CII. Onerous reporting and compliance mandates (e.g., audits, risk assessments, incident reporting) force businesses to divert scarce resources away from proactively managing evolving cyber risks in order to fulfill requirements that quickly become outdated. It may also inadvertently drive a culture of checking of boxes, creating an industry focused on compliance rather than a proactive and thoughtful approach that focusing on improving cybersecurity.

- **Cybersecurity incident reporting is distinct from cybersecurity threat sharing**. The former occurs after an incident happens and the damage is done, whereas the latter is proactive, informing organizations of potential threats (e.g., malicious code, indicators of compromise, tactics of cyber criminals) so that organizations can protect and defend their networks. While the draft bill mandates incident reporting, it is silent on cyber threat information sharing. A mechanism for information sharing should be added to the draft bill and should include the following parameters: multidirectional cyber threat sharing (e.g., government to industry, industry to industry); voluntary sharing of information; and protections from liability (including liability under data protection and anti-trust laws) when sharing information with industry peers or governments. Threat information sharing must protect privacy. Information sharing arrangements are most successful when they build on trust, enable bi-directional sharing, and enable victims of attacks to share information about both successful intrusions and near-miss attempts without fear of being investigated, sued, or held criminally liable as a result.

- **Mandatory and broad incident reporting requirements can be counterproductive.** Frameworks that force companies to report cybersecurity incidents without clearly defined risk-based criteria, leaving broad thresholds for reporting, can unintentionally inhibit cybersecurity by causing companies to over notify of *any* incident on their systems. This can lead to notification fatigue, increased costs, and operational distractions, which makes it difficult to identify and address the most important incidents. Additionally, it is unclear what the exact goals for incident reporting are and what CSA would do with the information once submitted.

- **Investigatory powers must be clearly defined and subject to checks and balances.** We urge the authors of the draft bill to limit officials' investigatory powers to only those systems that have been directly impacted by, or are suspected to have propagated, an incident which significantly impacts the continuity of essential services. We further urge the government to ensure that there are appropriate checks and balances in place to guard against the abuse of investigatory powers.

- **Criminal liability under the draft bill penalizes the wrong actors.** Criminal liability should be reserved for perpetrators of attacks, not CII owners. Not only do such penalties punish the wrong actor, they create a *significant* disincentive for investment in Singapore. Regulatory agencies should rely on specific directions to CII owners, with fines or injunctive relief as a means to promote compliance.

- **Licensing cybersecurity providers and professionals is problematic.** We recommend eliminating the licensing requirement as it runs counter to the objective of developing of a vibrant cybersecurity ecosystem in Singapore. According to estimates, Singapore's cybersecurity industry has the potential to double in value by 2020[1] with the potential to provide more than 2,500 additional job openings by 2018.[2] The proposed licensing requirements, however, lack transparent and established eligibility criteria, create burdensome jurisdictional complexities that could increase the difficulty and cost for international firms, and could hamper the development of a vibrant cybersecurity ecosystem in Singapore. An industry-led effort is better suited to keep pace with the technological changes. Companies offering cybersecurity services must offer high-quality and effective security solutions in order to effectively compete in the market, and most companies adhere to global best practices.

- **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. As Singapore moves forward with finalizing and implementing this law, any changes to codes of practice, standards, incident reporting, licensable servicers, and essential services should include a public consultation before amendments are made.

The attached table explains our concerns in greater detail, seeks clarification on several provisions, and offers our recommendations.

Cyber secure and resilient economies do not come about as a result of top-down legislation or regulation. Singapore 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.

Signed,

The American Chamber of Commerce in Singapore
BSA | The Software Alliance
Coalition of Services Industries
Information Technology Industry Council
US-ASEAN Business Council
U.S. Chamber of Commerce

[1] *Singapore Cybersecurity Strategy*. October 10, 2016. http://bit.ly/2ej1KEl
[2] Channel NewsASIA. *Cybersecurity sector projected to grow to S$900m by 2020: Yaacob*. March 22, 2017. http://bit.ly/2wySl3Q

Section No.	Issue	Comment
2(1) 7	Interpretation and designation of CII	There are several ambiguities concerning how the term critical information infrastructure is defined and used throughout the draft bill. In general, we seek two critical clarifications: ***(1) Clarify that only those systems designated as CII by the Commissioner (pursuant to Section 7) will be subject to the requirements of the draft bill.*** As presently drafted, it is unclear whether all systems that meet the definition of CII in Section 2 are subject to the requirements of the draft bill, or if the requirements apply only to systems owned by essential services that are designated as CII by the Commissioner pursuant to the Section 7 procedures. We presume that the intention is to limit the obligations to owners of systems deemed CII by the Commissioner, and that the Section 2 definition of CII is intended to serve as the criteria (referenced in Section 7(1)(a)) by which the Commissioner will evaluate whether a system owned by an essential service, identified in the First Schedule, should be deemed CII. We urge additional clarity on this point. To resolve this ambiguity, we recommend that the definition of critical information infrastructure be amended as follows: *critical information infrastructure means a computer or a computer system <u>DESIGNATED BY THE COMMISSIONER PURSUANT TO SECTION 7</u> that is necessary for the continuous delivery of essential services which Singapore relies on, the loss or compromise of which will lead to debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.* In addition, considering the distributed nature of information infrastructure and the complexity in determining the responsibilities and ownership as defined by this bill, we recommend that CII owners be given a minimum of 45 days to review the notice and submit representation against the designation or coordinate internally and, as per Section 7(4)(b), appoint a contact person who can represent the CII owners in all matters arising around audits, queries, reporting and so on. [*Continued on page 6.*]

Section No.	Issue	Comment
2(1) 7	Interpretation and designation of CII	***(2) Clarify that CII Owner refers to the provider of essential services (and not third-party Information and Communications Technology (ICT) service providers)*** We likewise seek clarification that compliance with the draft bill, and any ensuing codes of practice, is the responsibility of entities that provide the essential services identified in the First Schedule. The current definition of owner of critical information infrastructure could be read to suggest that the owner of any third-party service that provides IT support to an essential service would be directly subject to the requirements of the draft bill. Such an outcome would bring a massive new class of companies under the oversight of the Commissioner. It would be inappropriate to impose many of the specific requirements of the draft bill on companies that do not themselves provide the essential services to the Singaporean public. Such overreach would not result in better security outcomes. In fact, it could deter the providers of cutting-edge security services from entering into business relationships with Singapore's essential service providers. A better approach is to clarify that providers of essential services are responsible for complying with the draft bill and that they should pass along any applicable requirements through contractual arrangements with their third-party service providers.
2(1)	Interpretation and designation of CII	In general, definitions provide clarity. Clarity is sought on the definitions for the following: (1) What is debilitating impact in the context of loss or compromise of an essential service? In particular, does it look at the impact to the service and/or those relying on the service?
5	Duties and functions of Commissioner of Cybersecurity	We have a number of concerns when it comes to the duties and functions of the Commissioner: (1) Section 5(a) appears to extend the Commissioner's powers to all computers and computer systems. It should be confined to CII. (2) Regulators should be required to rely on and promote the adoption and use of globally accepted standards and specifications relevant to the security of computers and computer systems. (3) Cybersecurity laws and regulations already exist in Singapore. Regulators of some CII sectors already have powers to enforce cybersecurity obligations. The draft bill should clearly articulate that the Commissioner has the duty to ensure consistency and harmonization among existing sectoral regulations, the draft bill, and any new codes of practices, standards, or regulations. (4) It is important to acknowledge that the Commissioner should cooperate closely with the private sector in any development of regulations or standards, and rely on their best practices. Language should be added whereby the Commissioner would have a duty to promote, develop, maintain, and improve communication and coordination with sectoral regulators. For instance, the Commissioner should be required to share cyber incident information across agencies to improve situational awareness and prevent redundant reporting requirements. Incident information should be protected from disclosure according to Section 48.

Section No.	Issue	Comment
8 10 11 13 14 20 24 Others	Provision of information	The scope of the information gathering powers envisaged by the draft bill are very broad and could potentially require CII owners and operators to reveal sensitive confidential and proprietary information (e.g., network system technical information, source code). We request clarification that the revelation of such information is not required and to the extent such information must be disclosed, adequate obligations of confidentiality and non-use. We seek modification to Section 8 and 24. Requirements to compel organizations to divulge their intellectual property (IP) without binding assurances that their IP will be protected will inhibit industries and innovators from bringing the best technologies and practices to Singapore. Detailed design and implementation information relating to computers are IP, which for-profit organizations rely upon to ensure business success. CII may host data pertaining to persons in Singapore and of other jurisdictions especially in the case of multinational organizations. The draft bill should have an explicit provision that inter-jurisdictional approvals from relevant authorities will be obtained by the industry regulator or by the Commissioner.
8(2) 11	Technical information	We request greater clarity on what comprises technical information, as used in Section 8(2) and how this relates to the various categories of information in Section 11.
10	Duties of owner of critical information infrastructure- add reference to prevention	Per the Public Consultation Paper, MCI/CSA aims for the law to take a "proactive approach for CII protection." The paper also states that "the owner of each computer should be responsible for ensuring that the computer is well-protected." However, the draft does not encourage CII owners to undertake prevention activities to protect CII from cyberattacks. Per Section 10, CII owner duties include undergoing audits and carrying out risk assessments. Language should be added here recommending CII owners to put in place prevention capabilities where possible.
10(b)	Compliance with codes of practice, standards of performance or directions.	It is unclear whether the obligation to comply with codes of practice, standards, performance, and directions extends to the parts of CII that are not wholly located in Singapore. We recommend clarifying that the obligation only pertains to the parts of CII within Singapore.
10(c) 15	Duties of CII owners – cybersecurity incident reporting	The obligation to report a cybersecurity incident should be confined to incidents that have a *significant* impact on the continuity of essential services, as per Section 15. Section 10(c), which appears to require the reporting of any cybersecurity incident, has the potential to result in notification fatigue and make it difficult for the Commissioner to distinguish and identify incidents that require more immediate action.

Section No.	Issue	Comment
10(c) 11(5) 15 17 21	"Cybersecurity incident" vs "significant/serious cybersecurity incident"	We note that the reporting requirements under Sections 10(c) and 11(5) are triggered upon the occurrence of *any* cybersecurity incident impacting CII. In contrast, the reporting requirements under Sections 15 and 17 are triggered upon the occurrence of any *significant* cybersecurity incident. We seek clarification on what constitutes a *significant* cybersecurity incident, especially for purposes of incident reporting. Concerning the definition of serious cybersecurity incident in Section 21(2): (1) The severity schema in Section 21(2) is vague and requires additional detail (e.g., risk of significant harm, risk of disruption, number of computers). We recommend deleting the reference to value of information, as this is highly subjective and very hard to independently verify, especially when considering that the overall provision in which it appears—investigation of serious cybersecurity incidents—would tend to suggest urgent action. (2) We also recommend confining it to any incident resulting in, or an attempt to cause an incident that if successful would have resulted in, either: (a) the exfiltration of data that is essential to the operation of critical cyber infrastructure; or (b) the defeat of an operational control or technical control, essential to the security or operation of critical cyber infrastructure. We further recommend incorporating the following factors which are drawn from the European Union's Directive on security of network and information systems (NIS Directive)[3], for determining the severity of the incident: • The number of users relying on the essential services provided by the entity concerned; • The dependency of other essential services on the service provided by the entity; • The impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; • The market share of the entity; • The geographic spread with regard to the area that could be affected by an incident; and • The importance of the entity for maintaining a sufficient level of the essential service, taking into account the availability of alternatives for the provision of that service.

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council. http://bit.ly/2azjoxJ

Section No.	Issue	Comment
10(c)(ii) 11(1)(b) 11(1)(c) 15(1)(b)	Duties of CII owners with regard to interconnected computers or computer systems	The scope is unclear with regard to the obligations of CII owners as they relate to "any computer or computer system … interconnected with or communicates with the critical information infrastructure." This potentially causes the information provision obligations of CII owners under the draft bill to be unduly broad. It could include, for example, extend to computers and computer systems that are subject to the laws of other jurisdictions, under which CII owners could face liability if information (e.g., personal data) is disclosed in Singapore. We therefore recommend removing the concept of interconnected computers from the information provision obligations of CII owners under the draft bill. Should the drafters of the draft bill nonetheless desire to retain this concept, we recommend that it include only direct connections and communications, and exclude transitive and/or indirectly related communications and connections. We also request clarification on the scope and/or consideration of materiality as it relates to any obligations on non-CII designated system(s). Otherwise, these sections risk being interpreted too broadly as to create unduly onerous burdens on infrastructure owners while proving ineffective at protecting CII.
10(d) 10(e) 13(2)(b) 16	Duties of CII owners - cybersecurity audits and risk assessments of CII	While cybersecurity audits are important for cybersecurity assurance, they do not ensure cybersecurity. The government should also work with the owners and operators of CII to identify other avenues for cybersecurity assurance, including voluntary arrangements with CII owners and/or operators. Where reliance is placed on audits, it would be important to rely on and promote the adoption and use of globally accepted standards such as the ISO/IEC 27000 family of information security management systems standards or the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. The Commissioner should also accept evidence or results of a security audit performed by a qualified third-party auditor, including any auditor who is internationally-accredited, and undertaken by CII owners of their own volition on a regular basis independent of any obligation to do so under the draft bill. As typical audits of critical systems involve collection, analysis, and reporting on multiple aspects depending on the size and complexity, a CII owner may receive the report anywhere from 30 to 90 days after the audit is completed. Since this factor is out of control of the CII owner, we recommend that the requirement to share the report with the Commissioner be changed from "30 days after completion of the audit" to "30 days within receipt of the report." This change will also allow the CII owner to review the findings and share a comprehensive plan of remediation with the Commissioner.
10(f) 17	Duties of CII owners – participation in cybersecurity exercises	Cybersecurity exercises are important ways to raise the level of readiness across sectors, build incident response plans and capabilities, and improve communication and coordination between the CII operators and government agencies. However, we urge that participation in comprehensive cybersecurity exercises remain voluntary.

Section No.	Issue	Comment
10 11 12 15 16	Notifications by financial organizations	Financial organizations regulated under the Monetary Authority of Singapore (MAS) are already obliged to notify MAS of material changes and cybersecurity incidents. The draft bill requires financial organizations to duplicate processes for notifications and communications into multiple agencies. Coordinating notifications and communications via the sectoral regulator (e.g., MAS for financial organizations) during cybersecurity incidents and events would be a better approach.
11(2) 11(5)	Notification of and definition of material change	What constitutes a material change to CII is unclear. While there is a definition of material change in Section 11(5), which relies on the effect on the cybersecurity of the CII or the ability of the CII owner to respond to cybersecurity incidents, there are no specified conditions, whether quantitative or qualitative, that these effects have to be considered material in nature. We request a clearer definition of material change.
11(4) 20(5) 24(7)	Immunity for provision of information	We support the immunity provided in Sections 11(4), 20(5), and 24(7) regarding obligations of confidentiality. We recommend the addition of a general provision to provide immunity for the voluntary disclosure of information, in good faith, relating to a cybersecurity threat or a cybersecurity incident to the Commissioner and other parties who have been given information gathering powers and sharing under the draft bill. Such immunity should be limited to covering only the particular act of disclosure and not any other noncompliance with law to prevent abuse of such provisions. We also suggest that the safeguards in Sections 11(4) and 20(5) be made applicable whenever there is a requirement for a CII owner or any person to provide information or access to systems (e.g., under Sections 15, 16, 21, and 24). Notwithstanding these safeguards, a CII owner may still be held liable in foreign jurisdictions, especially where such disclosure runs afoul of foreign law. For this reason, we would suggest that the exception in Section 11(3) be similarly made applicable to all instances where a CII owner is required to disclose information or provide access to systems, and that written law expressly include applicable foreign law: "(3) The owner to whom a notice is issued under subsection (1) is not obliged to disclose any information where the owner is prohibited by any written law from disclosing such information."

Section No.	Issue	Comment
12	Codes of practice or standards of performance	We urge the government to work with the private sector to develop codes of practice and standards and to put in place measures and enable capabilities that can assist in the detection of, recovery from, and investigation of incidents. Standards and best practices are optimally created in close collaboration with the private sector and used on a voluntary basis and most effective when developed and recognized globally. Policymakers should align practices and standards with industry-backed approaches to information security controls and risk management, such as the ISO/IEC 27000 family of information security management systems standards or the U.S. National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*. Of note is a proposal to develop an ISO/IEC standard built around the Framework's approach to risk management (see ISO/IEC PDTR 27013). The Commissioner should also ensure that cybersecurity codes of practice and standards are harmonized with any existing sectoral regulations. This is consistent with the desired outcome of the draft bill, which applies a harmonized risk-based cybersecurity framework across sectors.
14	Change in ownership of critical information infrastructure	What constitutes a change of ownership of CII is not specified in the draft bill. Further, it is unclear whether the section applies to a change in ownership in a part of CII, or to parts of CII that are outside Singapore. Due to sensitivity around personnel changes and other constraints, we recommend that the reporting requirement be changed from "90 days before the change" to "not later than 30 days after the change." We request a clearer definition of change of ownership and further clarity over what triggers the obligations under Section 14(1).
15	Reporting requirements and prescribed period for cybersecurity incident reporting	Rather than prescribing a specific timeline, we recommend that the obligation be to report the incident as soon as reasonably possible.
16	Frequency of cybersecurity audits and risk assessments	The need for and frequencies of cybersecurity audits and risk assessments should be risk-based and not artificially prescribed. The owner of the CII should have a say determining the need, scope, and frequency of cybersecurity audits and risk assessments.

Section No.	Issue	Comment
20 21	Powers to investigate and prevent cybersecurity incidents and serious cybersecurity incidents	We are concerned about provisions in draft bill that require businesses to comply with notices or directions issued by the commissioner (which, other than Sections 20 and 21, would also include various Sections in Part 3 of the draft bill), including providing access to premises and computers or information during investigations. The scope of the powers under Sections 20 and 21, in particular are too broad and lead to concerns on the subjective application of the law. Suggested changes: (1) Remove Section 21(1)(c)(iv) which allows investigating officers to install software programs onto a company's systems and computers. There are alternative methods to conduct investigations and we consider this clause excessively intrusive to any organization's systems. (2) Limit the scope of investigative access to only those systems that have been directly impacted by, or are suspected to have propagated, a cyberattack. (3) In lieu of having government officials conduct the investigation, allow the affected entity to engage a licensed third party to investigate affected systems and submit a report to the government. (4) Allow the investigated entity to redact or withhold sensitive confidential and proprietary information (e.g., network system technical information, source code, personally identifiable information unrelated or unnecessary to the investigation, and trade secrets). Please also see our comments on Sections 8, 11, etc. concerning the provision of information. In addition, and similar to our comments above on Sections 10(c)(ii), 11(1)(b), 11(1)(c), and 15(1)(b), the investigatory powers should be confined to only computers and computer systems (or parts thereof) located within Singapore. We also believe that the government should refrain from prescribing remedial measures, which is best left to industry cybersecurity professionals.
24	Emergency cybersecurity measures and requirements	The scope of this provision should be clarified to narrow officials' powers to gather information only for the purposes of preventing, detecting, or countering cyber threats. We also urge that emergency measures only be invoked when an attack poses an imminent an significant threat to wide-scale essential services interruption, or national security; or may cause major physical damage to property, bodily harm or death. We further urge this provision be limited to providing the authority to compel only information that is readily accessible.

Section No.	Issue	Comment
24(8) 48	Preservation of secrecy	We welcome the confidentiality safeguards in Sections 24(8) and 48 and recommend the following clarifications: (1) The draft bill should set forth the procedures that will apply to the Commissioner's acceptance or rejection, under Section 48(5), of a request for confidentiality. (2) The draft bill should provide a right of appeal in instances where the Commissioner has determined that it is necessary to disclose information pursuant to Section 48(5). (3) Whether information that is disclosed voluntarily is protected under Sections 24(8) and 48. In relation to point (1) above, we also request that the draft bill be amended to grant clearer confidentiality processes such as the following: • Prenotification where the Commissioner wishes to disclose commercially confidential information. • Grounds by which the Commissioner assesses the written statement or which the decision to disclose may be challenged. To avoid inadvertent disclosure loopholes, we also recommend that the obligation of confidentiality should extend beyond specified persons and cover any recipient of information that is disclosed under or for purposes of the draft bill. We further recommend that the obligations of confidentiality under Sections 24(8) and 48 be extended to information that is disclosed voluntarily.
25	Cybersecurity service providers	We request that the licensing requirements for cybersecurity providers be eliminated. Licensing requirements are onerous, costly, impede business and will have little impact on improving cybersecurity. We also expect this provision will increase operational costs for businesses, which could adversely affect the growth of Singapore's vibrant cybersecurity ecosystem and lead to a less secure ICT environment. In addition to cost increases, requiring licenses for individual practitioners may incentivize the most qualified practitioners to work elsewhere where such a license is not necessary. This could cause more harm than good to the defense and security of Singapore's CII. There is significant competition in the cybersecurity services marketplace that drives constant improvement of cybersecurity solutions available to different consumers. We recommend eliminating the licensing requirement, since companies offering cybersecurity services must offer high-quality and effective security solutions in order to effectively compete in the market.

Section No.	Issue	Comment
26 - 28	Licensing of cybersecurity service providers	While we recommend that the licensing requirement should be eliminated, the draft bill is unclear as to the scope of application of Sections 26 through 28, including, in particular, the exemption under Section 26(3). For example, we are unable to determine if the draft bill intends that cybersecurity service providers not located in Singapore, nor providing services to the Singapore market, should be required to hold licenses when working on part of a computer system that is physically located outside of Singapore. This is especially pertinent when that computer system is interconnected with CII, which would create burdensome jurisdictional complexities. In another example, we are unable to determine based on the draft bill if a subsidiary or affiliated company would be covered under the exemption in Section 26(3) when providing licensable cybersecurity services to another affiliate or company and no one else. We recommend that: (1) Again, the licensing requirement for managed security services be eliminated; (2) If the licensing requirement is maintained, the scope of providing licensable cybersecurity services be clarified with respect to foreign vendors and services; and The exemption in Section 26(3) be expanded to affiliated companies providing cybersecurity services to the rest of the companies within the corporate group.
53(c)	Retention of Service Records	There is a requirement in Section 53(c) to retain service records for five years, including client information, services provided, names of the employee who provided the service, etc. A document retention period of 5 years is burdensome and onerous. Furthermore, an enterprise customer would likely be subject to sector-specific data retention requirements. Therefore, imposing lengthy document retention requirements would lead to duplication of records. We suggest that sector-specific data retention requirements already in place should take precedence to avoid creating a superfluous retention obligation and where that does not exist, consider reducing the record retention timeline to a more reasonable length of time.

Section No.	Issue	Comment
First Schedule	Essential services	It is unclear whether banking and financial institutions offering services listed in the first schedule are considered CII or are other considerations taken into account (e.g., relative size of offering in market, interconnection with other elements of the local economy) to determine whether they have earned the CII designation. If other considerations exist, we request that these be clarified. By extension, if a banking and financial institution is determined to be CII, the connection of this designation with Notice 644.[4] We seek clarification on whether the scope of services in the first schedule overlaps with the Monetary Authority of Singapore's (MAS) view criticality in Notice 644 or vice versa. We would also like to request clarification on whether electronic wallets and e-commerce (e.g., stock exchanges) are considered one of the enumerated services in "services related to banking and finance?" and on what kinds of services can be considered to be related to these categories. Further, we request clarification whether all applications of the entity count as CII or only the ones used to provide the service in the First Schedule.
First Schedule and Second Schedule	Essential services and Licensable Cybersecurity Services	Since the Minister may directly amend the schedules, particularly the list of licensable services in the Second Schedule, there should be a public consultation before the amendments are made and a grace period granted for compliance. The draft bill should also clearly specify the criteria under which the Minister may modify the list of essential services and licensable cybersecurity services in the First Schedule and Second Schedule (to add new services to, or remove or modify existing services listed in, these schedules).
General	Regulatory harmonization	We seek clarification on whether the intent of the draft bill is to supersede other existing obligations, including but not limited to those in the following regulatory instruments: (1) The Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines. (2) MAS Notice CMGN02_2014. (3) MAS Notice 644. (4) The Private Security Industry Act (PSIA) (which requires a private investigator license for investigative services, which are arguably related to incident response and computer forensics). (5) The draft Singapore standard based on the Infocomm Media Development Authority's Cloud Outage Incident Response (COIR) Guidelines. In the event that the obligations are not intended to supersede, we request that the regulation be harmonized as much as possible with respect to both sets of regulators. We request that one harmonized set of cybersecurity regulations be set out for entities already subject to any existing sectoral regulations. Where possible, oversight and reporting should be administered through the regulator who oversees the institution's regulatory compliance. This will allow for a centralized approach to regulatory oversight and prevent multiple reporting to different agencies on the same matter.

[4] Monetary Authority of Singapore. *Notice 644 Technology Risk Management*. June 21, 2013. http://bit.ly/2vKetFR

Section No.	Issue	Comment
General	Criminal liability	Throughout the draft bill mention is made of criminal liability for willful noncompliance with jail sentences from 6 months to 2 years and an exceptional 10 years for certain offenses. Such criminal liability of this nature is disproportionate and, combined with personal liability for corporate officers, raises the cost of operations, insurance, and compliance, which dis-incentivizes companies to invest in Singapore. Criminal liability should be reserved for perpetrators of attacks, rather than those actors working to protect Singapore's critical infrastructure. Not only do such penalties punish the wrong party, they create a significant disincentive for investment in Singapore. We recommend that Singapore instead rely on fines or injunctive relief as a means to promote compliance. Further, we seek clarification on whether liability applies to individuals or companies.
General	Voluntary cyber threat information sharing	Absent from the provisions of the draft bill is meaningful language on the establishment of a framework for the voluntary sharing of cybersecurity information. We suggest the draft bill include a new section promoting voluntary cyber threat information sharing among the public and private sectors and between private sector entities. The most effective information-sharing frameworks guarantee private companies protections from liability (including liability under data protection and anti-trust laws) when sharing information with industry peers or governments on incidents, threats, vulnerabilities, and mitigations. Organizations that share cyber threat information should be given assurances that data provided will not be used for law enforcement purposes against them, and will be used only against the cyber attacker and/or for the prevention, detection, and response to cyberattacks. At the same time, governments and companies should take meaningful steps to ensure that personal information is not inappropriately shared.
General	Situational awareness	The draft bill advances the idea that government agencies must have an omniscient view of cybersecurity on computers and computer systems owned and operated by private companies. Cybersecurity is a shared responsibility between governments and companies with the balance not titled heavily in favor of one or another. We urge that the government of Singapore consider the costs and benefits of providing agencies the authority to access private companies computers and computer systems so easily.

The American Chamber of Commerce in Singapore (AmCham)
AmCham Singapore is the leading international business association in Singapore, with over 5,000 members representing more than 700 companies. American companies' direct investment in Singapore exceeds an estimated US$258 billion.

BSA | The Software Alliance
BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, D.C., and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

The Coalition of Services Industries
The Coalition of Services Industries (CSI) represents the interests of the dynamic American service economy, which employs over 75% of the workforce and generates 3/4 of national economic output. Since 1982, CSI has created greater public awareness of the major role services play in the U.S. economy, and it has shaped domestic and international economic policies on behalf of the services sector. The broad range and diversity of the U.S. service economy is reflected in CSI's membership, which includes major international companies from the banking, insurance, telecommunications, information technology, logistics and express delivery, audiovisual, retail, and other service industries. CSI members conduct business in all 50 states and in more than 100 countries.

The Information Technology Industry Council
ITI is the global voice of the tech sector. We advocate for public policies that advance innovation, open markets, and enable the transformational economic, societal, and commercial opportunities that our companies are creating. Our members represent the entire spectrum of technology: from internet companies, to hardware and networking equipment manufacturers, to software developers. ITI's diverse membership and expert staff provide a broad perspective and intelligent insight in confronting the implications and opportunities of policy activities around the world.

US-ASEAN Business Council
For over 30 years the US-ASEAN Business Council has been the premier advocacy organization for U.S. corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN). Worldwide, the councils 150-plus membership generates over $6 trillion in revenue and employs more than 13 million people. Members include the largest U.S. companies conducting business in ASEAN and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The council has offices in Washington, D.C.; New York, New York; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.

U.S. Chamber of Commerce
The U.S. Chamber of Commerce represents the interests of more than 3 million U.S. businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations. Its International Affairs Division includes more than 50 regional and policy experts and 23 country-specific business councils and initiatives. It also works closely with 116 American Chambers of Commerce abroad.