15 January 2024

BSA COMMENTS ON PROPOSED CYBERSECURITY (AMENDMENT) BILL 2023

Submitted Electronically to the Cyber Security Agency of Singapore

BSA | The Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the Cyber Security Agency of Singapore (**CSA**) on the draft Cybersecurity (Amendment) Bill 2023[2] (**Bill**) and the accompanying Public Consultation Paper[3] (**Consultation Paper**).

BSA recognises that increased connectivity, computing, and data storage needs creative solutions to maintain effective cybersecurity. We support Singapore's efforts to ensure that the Cybersecurity Act 2018 (**Cybersecurity Act**) remains fit-for-purpose and capable of addressing ever-evolving cyber threats. Cybersecurity is a shared responsibility across public and private stakeholders, and effective cybersecurity legislation requires close coordination between industry and government in both formulation and implementation.

Unfortunately, although CSA has discussed certain elements of the proposed amendments with some selected industry stakeholders, there are substantial portions of the proposed amendments that have not been subject to previous discussions. While many of the obligations in the Cybersecurity Act, including the proposed amendments, are imposed directly on "owners of critical information infrastructure", the requirements will impact so-called "owners" of non-provider-owned critical information infrastructure (**CII**). It is therefore disappointing that there has not been an adequate consultative process with such entities.

In this regard, BSA strongly urges CSA to undertake further discussions with key stakeholders, such as those organisations that may be deemed owners of non-provider-owned CII, on the issues enumerated below.

[1] BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software.

BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Draft Cybersecurity (Amendment) Bill 2023, December 2023, https://www.reach.gov.sg/docs/default-source/participate/public-consultation/cyber-security-agency-of-singapore-(csa)/cybersecurity-(amendment)-bill-2023_for-public-consultations.pdf.

[3] Public Consultation Paper on Draft Cybersecurity (Amendment) Bill 2023, December 2023, https://www.reach.gov.sg/docs/default-source/participate/public-consultation/cyber-security-agency-of-singapore-(csa)/public-consultations-paper---cybersecurity-amendment-bill.pdf

300 Beach Road
#30-06 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

Summary of BSA's Recommendations

Part 3A (Provider of Essential Service Responsible for Cybersecurity of Non-Provider-Owned Critical Information Infrastructure)

Part 3A creates obligations around a new category of assets referred to as "non-provider-owned critical information infrastructure and a new category of entities referred to as "owners of non-provider-owned critical information infrastructure". It is unclear why or how this new category is required when the Commissioner already has the ability to designate a "computer or computer system" as CII under Section 7 of the Cybersecurity Act.[4] Even a deemed "owner" may not be fully in control of the underlying systems it relies on (e.g., a provider of a software-enabled service or online service may operate on computing or network infrastructure owned and operated by other cloud and data centre providers). Because the concept of "ownership" of the asset, as opposed to the function, does not map well with complex commercial relationships between different software-enabled services and IT systems which a provider of essential services may be responsible for, it would be better to remove the new concept of "ownership" from the amendments altogether and retain the primary responsibility of managing relevant assets with the provider. If additional guidance is necessary for providers of essential services to better fulfil their obligations, these might be set out in advisory guidelines, similar to how other regulators in Singapore, such as the Monetary Authority of Singapore or the Personal Data Protection Commission, encourage their regulated entities to manage risk which may include those of other third party providers the entities may depend on.

If Part 3A is retained in the final legislation, it is important that the revised Cybersecurity Act:

1. Provide clear criteria for identifying non-provider-owned CII and owners of non-provider-owned CII (**Owners**).
2. Create a mechanism for the Commissioner consult directly with the asset's owner when ascertaining if an asset is a non-provider-owned CII.
3. Streamline processes in cases where multiple providers of essential services responsible for cybersecurity of non-provider-owned CII (**Providers**) use the same non-provider-owned CII.
4. Give Owners the right to appeal decisions by the Commissioner.

Part 3B (Major Foundational Digital Infrastructure Service)

5. Provide clear criteria for identifying major Foundational Digital Infrastructure (**FDI**) service providers.
6. Specify incidents which should be reported, timelines, and reporting requirements in the Bill.
7. Specify that "cloud computing service" in the context of FDI services refers to Infrastructure-as-a-Service.

Additional Comments

8. Incorporate principles of specificity and minimisation into requests for information.
9. Remain cognisant of precedent-setting effect in the region.

Part 3A (Provider of Essential Service Responsible for Cybersecurity of Non-Provider-Owned Critical Information Infrastructure)

Part 3A of the Bill addresses situations where the Providers make use of "non-provider-owned CII" from a computing vendor to provide essential services.[5] Under the proposed Part 3A, where Providers use non-provider-owned CII, the Providers are required to obtain legally binding commitments from

[4] Cybersecurity Act 2018 (No. 9 of 2018) at https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312

[5] Consultation Paper (2023), paras 5 and 7.

the Owners to ensure that the Providers can discharge their new duties[6] under the Cybersecurity Act. This arrangement between the Provider and Owner imposes substantial obligations on the Owners, albeit indirectly, many of which go beyond typical commercial arrangements. Among other things, the Owner will be contractually bound to give the Provider information on the Owner's CII upon request,[7] comply with any applicable codes or standards issued by the Commissioner,[8] as well as notify the Provider of any changes in beneficial or legal ownership of the Owner's CII.[9]

As BSA members create the technology solutions that power other businesses, including Providers, many of them may be deemed Owners under the proposed amendments and consequently subject to the above obligations. However, to our knowledge, CSA has not consulted or discussed with Owners their potential obligations under the proposed amendments, despite the Owners' important roles in the cybersecurity ecosystem.

As described above, due to Part 3A's ambiguity and the Commissioner's existing authority to designate a "computer or computing system" as a CII, and given that there has been, to our knowledge, limited consultation with the affected industry stakeholders regarding this new Part 3A, **we urge CSA to remove Part 3A from the proposed amendments and undertake further consultations with potential Owners. If Part 3A is retained in the Bill, our recommendations for Part 3A are as follows:**

1. Provide clear criteria for identifying non-provider-owned CII and their Owners

It is not clear how exactly the Commissioner will determine if a computer or computer system is a non-provider owned CII. The only stated criteria in the Bill is that the Commissioner must be satisfied that: a) the computer or computer system is "necessary for the continuous delivery of [an] essential service" and that the "loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore"; and b) the computer or computer system is "not owned by the provider of the essential service".[10] These criteria do not provide businesses with sufficient guidance. For example, it is not clear how the Commissioner will determine if a computer system is "necessary" for the delivery of an essential service, or what would constitute a "debilitating effect" on the availability of an essential service. This lack of guidance and transparency will create significant uncertainty among software service providers and information technology (**IT**) vendors, many of which provide a wide range of systems and services to companies which may be designated as Providers.

Furthermore, the interaction between different layers of "computer systems" that may be used by Providers adds complexity that the proposed legislation does not appear to recognise or address. For example, if a software service provider is deemed an "Owner" but does not control the computing or networking infrastructure it uses to provide its services, it is not clear how obligations that may be imposed upon the Owner by the Provider may be implemented.

As BSA has explained in past filings, expanding the scope of covered entities to include such service providers adds complexity without correspondingly enhancing cybersecurity. If CSA intends to expand

---

[6] Per the Consultation Paper (2023), para 7, these include duties to "a) provide the Commissioner with information on the non-provider-owned CII; b) comply with such codes of practice, standards of performance or written directions in relation to providers responsible for the non-provider-owned CII as may be issued by the Commissioner; c) notify the Commissioner of any change in the beneficial or legal ownership of the non-provider-owned CII; d) notify the Commissioner of any prescribed cybersecurity incident involving the non-provider-owned CII; e) cause regular audits of the compliance of the non-provider-owned CII with the Cybersecurity Act, codes of practice and standards of performance, to be carried out by an auditor approved by the Commissioner; f) cause regular risk assessments of the non-provider-owned CII to be carried out; and g) participate in cybersecurity exercises relating to the providers responsible for non-provider-owned CII as required by the Commissioner.

[7] Proposed Section 18AE in the Bill.

[8] Proposed Section 18AF in the Bill.

[9] Proposed Section 18AH in the Bill.

[10] Proposed Section 18AA in the Bill.

the scope of covered entities, the criteria for which entities may be considered Owners must be well defined.

Under the current Cybersecurity Code of Practice for Critical Information Infrastructure,[11] Section 3.7.3 already requires CII owners to conduct a cybersecurity risk assessment if they wish to implement "the whole or any part of the CII on cloud computing systems". This risk assessment can assist in determining whether a vendor is a non-provider-owned CII. However, more importantly, the Bill must provide a clear set of criteria for identifying non-provider-owned CII and their Owners. For example, under Australia's Security of Critical Infrastructure Act 2018 (**SOCI Act**),[12] a business is clearly an owner of a "critical data storage or processing asset" if its asset is used primarily to provide a data storage or processing service that relates to "business critical data" and is provided to an end user that is a government entity or another critical infrastructure asset.[13] This allows computing vendors to assess if they fall within the SOCI Act based on their customers and their services, and to execute their duties accordingly.

Recommendation: The Bill must provide clear criteria for identifying non-provider-owned CII and their Owners. This will enhance regulatory certainty and improve transparency.

2. Create a mechanism for the Commissioner to consult directly with an asset's owner when ascertaining if an asset is a non-provider-owned CII

The Bill vests the Commissioner with the power to obtain information from the Provider to ascertain if a computer or computer system fulfils the criteria of a non-provider-owned CII. Indeed, the Commissioner may request the Provider to furnish him with key details pertaining to said computer or computer system, such as "information related to the design of the computer or computing system".[14] This could be highly sensitive information that may be better communicated directly from the Owner to the Commissioner, rather than through the Provider.

As owners of assets that may be designated non-provider-owned CIIs, software service providers and IT vendors may be better-placed than Providers to furnish information on the function and design of these assets. While it is important to consult Providers to understand how these assets are deployed in the context of providing essential services, Providers may not have sufficient expertise to accurately explain how these assets are designed and function, as they neither own nor control these assets. Consequently, the Commissioner may be presented with incomplete or inaccurate information on important aspects of the assets, which will materially impact the Commissioner's decision to designate an asset as a non-provider-owned CII. An approach that involves enabling the Commissioner to interact directly with potential Owners will provide the Commissioner with a more comprehensive understanding of an asset before determining if it is a non-provider-owned CII.

Recommendation: Where the Commissioner "has reason to believe that a computer or computer system may fulfil the criteria in Section 18AA(2)", the Commissioner should be enabled to consult directly with the Owner or potential Owner regarding relevant information related to the computer or computer system. This will provide the Commissioner with a more comprehensive understanding of the asset before determining if it is a non-provider-owned CII.

---

[11] Cybersecurity Code of Practice for Critical Information Structure, July 2022 (last updated December 2022), https://www.csa.gov.sg/docs/default-source/legislation/ccop---second-edition_revision-one.pdf?sfvrsn=421a71ab_1.

[12] Security of Critical Infrastructure Act 2018 (SOCI Act) at https://www.legislation.gov.au/C2018A00029/latest/versions

[13] Section 12F of the SOCI Act 2018. The term "business critical data" is also separately defined as any of the following: a) personal information that relates to at least 20,000 individuals; b) information relating to any research and development in relation to a critical infrastructure asset; c) information relating to any systems needed to operate a critical infrastructure asset; d) information needed to operate a critical infrastructure asset; or e) information relating to risk management and business continuity in relation to a critical infrastructure asset.

[14] Proposed Section 18AB in the Bill.

3. Streamline processes in cases where multiple Providers use the same non-provider-owned CII

Multiple Providers may use the same non-provider-owned CII. As each Provider is required to secure binding legal commitments from the Owner that controls the non-provider-owned CII, a single Owner may receive multiple and redundant requests for information and audits, causing unnecessary administrative burdens and significantly compounding the resources required for Owners to discharge their obligations to their Providers.

CSA should work with Owners to streamline processes where multiple Providers use the same non-provider-owned CII. For example:

- Provider requirements on Owners should align with internationally recognised standards, such as the ISO 27001 series and SOC2 and SOC3. Owners should then be able to demonstrate compliance with their obligations by sharing documentation demonstrating their compliance with such standards.
- Owners should only be required to participate in a single, comprehensive audit once every 2 years.[15] Audits are highly resource intensive and multiple audit requests from Providers will lead to excessive burdens on an Owner's resources. A single comprehensive audit, demonstrating compliance with relevant internationally recognised standards, should be sufficient to provide the findings for all Providers using the same non-provider-owned CII.
- While it is not clear if Owners themselves need to participate in cybersecurity exercises,[16] to the extent that they are required to do so, there should be reasonable limits on the Owners' involvement in such exercises with different Providers that they serve.

<u>Recommendation</u>: CSA should work with Owners to streamline processes where multiple Providers use the same non-provider-owned CII. This will reduce unnecessary administrative and resource burdens placed on the Owners.

4. Give Owners the right to appeal decisions by the Commissioner

Section 18AM of the Bill allows a Provider to appeal to the Minister against the "decision, order, direction, provision or amendment" issued by the Commissioner in respect of any obligations in Part 3A. However, even though the Bill imposes substantial obligations on Owners indirectly by requiring the Provider to secure various legal commitments from Owners, the Owners are not afforded a similar right to appeal.

The lack of an appeal mechanism for Owners is particularly concerning in the context of the Commissioner's identification of non-provider-owned CII and their Owners. When issuing a notice designating a company as a Provider, the Commissioner will also identify the non-provider-owned CII and the "person who appears to be the owner of the non-provider-owned CII".[17] However, while the Bill allows a Provider to appeal against the Commissioner's designation,[18] there is no such avenue of appeal for Owners. As it stands, the Commissioner can identify a computer or computer system as a non-provider-owned CII without requesting information from or consulting the vendor of that system, and the vendor would not be able to appeal the Commissioner's decision. This runs counter to the core principles of due process and transparency.

<u>Recommendation</u>: The Bill should contain a mechanism for Owners of non-provider-owned CIIs to appeal decisions, orders, directions, provisions, or amendments issued by the

[15] Proposed Section 18AJ in the Bill.

[16] Proposed Section 18AL in the Bill.

[17] Proposed Section 18AA in the Bill.

[18] Proposed Section 18AM in the Bill.

Commissioner in respect of any obligations in Part 3A, including the Commissioner's identification of non-provider-owned CIIs and their Owners.

Part 3B (Major Foundational Digital Infrastructure Service)

Part 3B of the Bill covers providers of major digital infrastructure services of a foundational nature (i.e., Foundational Digital Infrastructure (**FDI**)). Under the proposed Part 3B, the Commissioner will specify the types of services that would be regulated as FDI services and designate providers of FDI services as major FDI service providers if he is satisfied that certain criteria are fulfilled, upon which these major FDI service providers will be "subject to several duties", including duties to: a) provide the Commissioner with information related to the cybersecurity of the major FDI; (b) comply with such codes of practice, standards of performance, or written directions in relation to the major FDI as may be issued or approved by the Commissioner; and c) notify the Commissioner of any prescribed cybersecurity incident.[19]

BSA supports CSA's risk-based approach of focusing on major FDI service providers. However, the Bill omits several important details, including the specific criteria for identifying major FDI service providers and timelines for incident reporting. While the Consultation Paper states that some of these details, such as the incident reporting requirements, will be developed pursuant to further stakeholder consultations,[20] Part 3B's lack of specificity will create substantial uncertainty among businesses who provide FDI services. **Our recommendations on Part 3B are as follows:**

5. Provide clear criteria for identifying major FDI service providers

It is not clear how the Commissioner will designate an FDI service provider as a major FDI service provider. The Commissioner can designate an FDI service provider as a major FDI service provider if: a) it provides an FDI service to or from Singapore; and b) the "loss or impairment" of the FDI service could disrupt the operations of "a large number of businesses or organisations in Singapore" which rely on the FDI service.[21] The above criteria do not adequately explain or provide certainty on the basis for which an FDI service provider will be deemed a major FDI service provider. Notably, the Commissioner is free to determine what is "a large number of businesses or organisations in Singapore" and the severity of an incident which would constitute "loss or impairment" of the FDI service.

The lack of clear criteria has substantial implications on business operations. For example, the Commissioner has the power to require "any person who appears to be a provider of [an FDI] service" to furnish information relating to the service for purposes of ascertaining whether the service provider fulfils the criteria for a major FDI service provider. As there are no clear objective criteria, the Commissioner can require the service provider to disclose all manner of sensitive information related to its services, even if such information may only be tangentially relevant. Clear criteria will reduce the potential burden on businesses to furnish information, while also serving as important guidance to the Commissioner regarding information he may reasonably request. Furthermore, given that the Bill allows service providers designated as major FDI services providers to appeal the designation,[22] clear criteria will facilitate the Minister's and Appeals Advisory Panel's consideration of the appeal.

<u>Recommendation</u>: CSA should clearly stipulate the criteria that would be used to determine if a service provider is a major FDI service provider in the Cybersecurity Act. Such criteria should include, but need not be limited to, the following:

- **Domestic user base size;**
- **Types of users serviced (e.g., whether CII owners use the service);**

[19] Consultation Paper (2023), para 20.

[20] Consultation Paper (2023), para 22.

[21] Proposed Section 18BB in the Bill and Consultation Paper, para 19.

[22] Proposed Section 18BJ in the Bill.

- **Domestic market share and revenue;**
- **Sensitivity of data handled; and**
- **Service exclusivity (i.e., whether the service offers functions that are not easily replicable/substitutable).**

No single criterion should be determinative of whether a service provider is a major FDI service provider – the criteria should be assessed holistically in line with a risk-based approach, and designations of major FDI service providers should be revisited periodically.

6. Specify incidents which should be reported, timelines, and reporting requirements in the Bill

Major FDI service providers are required to notify the Commissioner when a "prescribed cybersecurity incident" occurs. However, the Bill does not specify what would constitute a prescribed cybersecurity incident, save that these incidents either a) result in a disruption or degradation to the continuous delivery of the FDI service that the major FDI service provider provides in Singapore; or b) has a significant impact on the major FDI service provider's business operations in Singapore.[23] The Consultation Paper notes that the "[o]perational details of the incident reporting requirements will be developed in consultation with stakeholders and with reference to international practices", and that these would include "the list of cybersecurity incidents to be prescribed, the threshold (e.g., significance of an incident) for when a report becomes obligatory, the reporting timelines, and the information to be reported".[24]

Given the increasing costs of cyber security incidents, the reporting requirements should also focus on demonstrably measuring and improving cybersecurity. The outcome of the Bill, and implementing rules, should ultimately be assessed by how information from these reported cyber incidents is analyzed, enriched, and disseminated - ideally in a de-identified or anonymized manner - to bolster the security of the broader cyber ecosystem. This would help ensure that reported incident information is used to develop actionable intelligence that is rapidly pushed out to protect entities in real-time.

BSA appreciates that these details will be co-developed with industry stakeholders. However, it is not clear why they "will be set out separately, either in subsidiary legislation or administrative guidelines" — these details are critically important as they dictate how major FDI service providers should execute their obligations under the Cybersecurity Act. To the extent possible, any reporting requirements should be harmonized to align with globally emerging standards.

In our recommendations to the United States Cybersecurity and Infrastructure Agency (**CISA**),[25] we urged CISA to:

1. Narrow and harmonise the definition of "covered cyber incident" by defining such an incident as one that has caused substantial operational disruption or financial losses for the entity or has caused considerable material or non-material losses.

2. Include minimal, but specific reporting requirements to avoid encouraging covered entities from prematurely focusing on activities that do not advance the response to the incident.

3. Require a covered entity to report a covered incident no sooner than 72 hours from when the entity has a reasonable belief that it is the victim of a covered incident.

<u>Recommendation</u>: Given the importance of specifying the incidents which should be reported, the reporting timeline, and other reporting requirements (e.g., information to be included in the

[23] Proposed Section 18BI in the Bill.

[24] Consultation Paper (2023), para 22.

[25] US: BSA Response to the Cybersecurity and Infrastructure Security Agency (CISA) Request for Information on Implementing the Cyber Incident Reporting for Critical Infrastructure Act, November 14, 2022 at https://www.bsa.org/files/policy-filings/11142022cisacircia.pdf

report), these details should be specified in the Bill and form part of the main legislation. CSA should also co-develop these details with industry stakeholders and extend the public consultation as necessary to do so.

7. Specify that "cloud computing service" in the context of FDI services refers to Infrastructure-as-a-Service

The Bill states that an FDI service is one that "promotes the availability, latency, throughput or security of digital services",[26] and specifies that a "cloud computing service" may be an FDI service.[27] "Cloud computing service" is further defined as "a service, delivered from a computer or computer system in Singapore or outside Singapore, that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations".[28]

BSA notes that CSA's policy focus here is on "infrastructural services of a foundational nature"[29] (emphasis added). However, the definition of cloud computing service does not make any reference to the provision of digital infrastructure. As the current definition of cloud computing service can potentially encompass a wide range of digital services available online, CSA should state in the definition of cloud computing service that it refers specifically to Infrastructure-as-a-Service (**IaaS**), which provide the underlying digital infrastructure necessary for hosting applications, managing data, and delivering services.

Recommendation: CSA should state in the definition of cloud computing service that the term "cloud computing service" refers specifically to IaaS.

Additional Comments

8. Incorporate principles of specificity and minimisation into requests for information

The Bill contemplates many instances where information will be requested of a party. The Commissioner has powers to request a broad range of information directly from multiple stakeholders, including Providers (of essential services) and potential major FDI service providers. Providers, in turn, are required to contract with Owners (of non-provider-owned CII) so that Owners will furnish Providers with information on the non-provider-owned CII when the Commissioner asks the Provider to obtain such information.

Most of the information requested will be sensitive in nature. As such, the Cybersecurity Act should impose safeguards to protect the information disclosed. One important safeguard is to ensure that requests for information are as specific and narrowly targeted as possible. This is also why it is essential to implement clear criteria for matters which will invite such requests for information (e.g., the Commissioner requesting information to identify non-provider-owned CIIs and their Owners, or to identify major FDI service providers), as it will ensure that the requests for information are specific to the criteria.

Another important safeguard is to adopt minimisation procedures in connection with requests for information. This ensures that only relevant data is produced and used in response to a request. Such procedures should also be applied to the processing, retention, and dissemination of the information acquired through requests, to ensure that: a) the information acquired in the request is returned or destroyed if not relevant to the specific matter for which it was requested; b) such information is only used for lawful purposes; and c) the information is secured against unauthorised access or disclosure.

---

[26] Proposed amendment of Section 2 in the Bill.

[27] Proposed Third Schedule in the Bill.

[28] Proposed Third Schedule in the Bill.

[29] Consultation Paper (2023), para 17.

Again, clear criteria for matters which will invite requests for information will help to ensure that only relevant information is obtained and retained.

<u>Recommendation</u>: CSA should ensure that principles of specificity and minimisation apply to requests for information in the Bill. In this regard, it is crucial to introduce clear criteria for matters which will invite requests for information (e.g., identifying non-provider owned CIIs and their Owners, or identifying major FDI service providers).

9. Remain cognisant of precedent-setting effect in the region

Singapore is a global thought leader on cybersecurity policy. As such, CSA's approach to various issues in the Cybersecurity Act review, such as the regulation of non-provider-owned CII and major FDI services, will become a point of reference for other countries. This is especially so in the South-East Asian region, where Singapore's cybersecurity policies and approach are studied closely. However, many of these countries do not work closely with industry stakeholders, nor do they operate with the same restraint and consideration for industry stakeholders. For example, while the Commissioner in Singapore may exercise wide powers in a fair and just manner, the counterpart in another country may adopt the same powers but use them in a more arbitrary fashion, without consideration for the resource and administrative burdens imposed on industry.

<u>Recommendation</u>: We urge Singapore to remain cognisant of the precedent-setting effect that amendments to the Cybersecurity Act may have on the global cybersecurity landscape. Obligations should be clear and specific, while powers should be subject to necessary safeguards and oversight. Industry should be consulted frequently and rigorously.

Conclusion

We hope that our comments will assist CSA in its deliberations on the Cybersecurity Act. We look forward to serving as a resource as you continue to engage with industry. Please do not hesitate to contact me if you have any questions regarding this submission or if I can be of further assistance.

Sincerely,

Tham Shen Hong
Manager, Policy – APAC