17 July 2026

BSA COMMENTS ON PUBLIC CONSULTATION ON DRAFT DIGITAL INFRASTRUCTURE BILL

Submitted Electronically to the Ministry of Digital Development and Information, and the Infocomm Media Development Authority

The Business Software Alliance (**BSA**)[1] appreciates the opportunity to comment on the public consultation on the draft Digital Infrastructure Bill (**Bill**) by the Ministry of Digital Development and Information (**MDDI**) and the Infocomm Media Development Authority (**IMDA**). BSA is the global trade association of the enterprise software industry. Our members are leaders in AI, cybersecurity, cloud computing, and other cutting-edge technologies. We value our longstanding engagement with the MDDI and the IMDA and welcome the opportunity to share perspectives from the enterprise software industry.

BSA supports Singapore's objective of strengthening the security and resilience of the digital infrastructure that underpins its digital economy. We also recognise and appreciate the extensive engagement that IMDA has undertaken with industry in developing the Bill, including the briefing provided to BSA members on 18 May 2026. Many features of the Bill reflect that engagement, including the quantitative thresholds used to scope the licensing regime.

Singapore is a global thought leader on digital policy, and its regulatory frameworks are studied closely and often emulated by other jurisdictions, especially in Southeast Asia. The Bill is therefore a significant opportunity to set a positive precedent for the region: one in which obligations are clearly scoped and defined, regulatory powers are subject to appropriate safeguards and oversight, and industry is consulted meaningfully throughout. Conversely, provisions that are overbroad or open-ended risk being replicated elsewhere without the restraint with which Singapore's regulators customarily exercise their powers.

Our comments focus on three areas where the Bill would benefit from greater precision and stronger procedural safeguards. Well-defined obligations are easier to comply with and easier to enforce; overbroad or open-ended provisions, by contrast, risk diminishing Singapore's attractiveness as a destination for digital investment without necessarily delivering better security outcomes.

[1] BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

Software-as-a-Service Exclusion

BSA commends the MDDI and the IMDA for expressly excluding Software-as-a-Service (**SaaS**) from the definition of a regulated Cloud Computing Service in the Schedule to the Bill. This is consistent with what IMDA communicated at its meeting with BSA members on 18 May 2026, and with IMDA's stated policy focus on the infrastructure and platform layers. The use of clear, objective thresholds — a critical IT load of at least 10 megawatts for data centre facility services, and annual revenue of at least S$100 million from users in Singapore for Infrastructure-as-a-Service (**IaaS**) and Platform-as-a-Service (**PaaS**) offerings — provides welcome regulatory certainty and reflects the risk-based approach that BSA has advocated.

The SaaS exclusion is housed in the Schedule rather than in the body of the Bill, and Clause 58 empowers the Minister to amend the Schedule by order in the Gazette. As drafted, the scope of the licensing regime, including the exclusion of SaaS, could therefore be changed without the full parliamentary scrutiny that accompanies primary legislation.

Recommendation: BSA recommends that the Bill require consultation with industry prior to any amendment of the Schedule. This is especially important for any amendment that would expand the scope of the regime, in particular any change that would bring SaaS within scope. Prior consultation would give affected providers the opportunity to provide input on the necessity, design, and implementation timeline of any scope change, and is consistent with the collaborative approach that has characterised the development of the Bill to date.

Emergency Powers

Clause 18 confers on the Minister very broad powers to issue directions in an emergency. These directions may be issued not only to licensees but to any person or organisation; they may require the handover of sensitive information, including real-time information and information relating to the design and configuration of systems; and they override obligations of confidentiality, including contractual obligations owed to customers (Clause 18(3)(b)). Non-compliance is a criminal offence punishable by substantial fines and imprisonment of up to 10 years.

BSA recognises that governments require effective tools to respond to genuine emergencies. However, Clause 18 exposes an unlimited range of persons to whom directions may be issued to severe criminal penalties. This creates significant uncertainty for businesses, including those that are otherwise outside the scope of the licensing regime. Emergency powers of this nature should be tightly scoped to the situations that genuinely warrant them and should be accompanied by procedural safeguards commensurate with the level of intrusiveness.

Recommendation: BSA recommends that:

- Clause 18 should be scoped narrowly, so that directed measures in an emergency are necessary, proportionate, and directly linked to addressing the threat;
- The Bill should provide an avenue for persons subject to a direction under clause 18 to seek review of, or appeal against, the direction once the emergency has been addressed, so that the exercise of these powers is subject to meaningful ex-post scrutiny; and

- The Bill should confine criminal liability under clause 18 to intentional or reckless non-compliance, with an express defence where non-compliance is attributable to technical or operational inability to comply; and that lesser instances of non-compliance be addressed through administrative penalties consistent with a graduated enforcement approach.

Conclusion

BSA appreciates the opportunity to provide comments on the Bill and hopes that our comments will assist the IMDA in refining the Bill to meet the goal of resilience and security in the cloud ecosystem. We look forward to continuing our engagement with the IMDA on these issues and remain available as a resource as the DIA is finalised.

Yours sincerely,

Wong Wai San
Director, Policy – APAC