Industry Consultation on The Licensing Framework for Cybersecurity Service Providers

Comments from BSA | The Software Alliance

15 October 2021

Introduction

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments to the Cyber Security Agency of Singapore (**CSA**) regarding the proposed licence conditions and draft subsidiary legislation under the licensing framework for cybersecurity service providers found in Part 5 of the Cybersecurity Act.

BSA 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, providing the products and services that power other businesses. BSA members create the technology products and services that power other businesses. Our members offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. Our members are also leaders in security, having pioneered many of the software security best practices used throughout the industry today.

Since the implementation of the Cybersecurity Act in 2018, CSA has worked towards raising the awareness and encouraging the adoption of cybersecurity solutions by businesses. The licensing framework will be another pillar supporting CSA's work and it seeks to: i) provide greater assurance of security and safety to consumers; ii) improve the standards and standing of cybersecurity service providers; and, iii) address the information asymmetry between consumers and the cybersecurity service providers.

At the outset, we would like to express our appreciation to CSA for taking into consideration the feedback provided by industry during the previous industry consultation in August 2017, and

[1] BSA's members include: Adobe, Altium, Atlassian, Autodesk, AVEVA, Amazon Web Services, Bentley Systems, Box, Cisco, Dassault Systems, DocuSign, IBM, Informatica, Intel, Mastercam, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell Automation, Salesforce, ServiceNow, Shopify, Siemens PLM Software, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Unity, Workday, Zendesk, and, Zoom.

300 Beach Road
#30-06 The Concourse
Singapore 19955

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

Regional Representative Office
UEN: S97RF0005K

incorporating some of the feedback in the current proposals. This notwithstanding, we remain deeply concerned about the precedent-setting effect of the proposed licensing framework on cybersecurity in Singapore as well as the wider global cybersecurity industry.

Our recommendations, discussed in greater detail below, address the following topics:

- Clearer exemptions under licensing requirements
- Licensing requirements for third-party service providers
- Provision of information
- Schedule of licensable services

Our comments are aimed at ensuring the proposed licensing framework and the draft subsidiary legislation (**SL**) can effectively achieve the objectives of CSA, in a manner that is risk-based and outcome-oriented while keeping pace with technological developments.

Recommendations

Clearer Exemptions under Licensing Requirements

BSA welcomes and appreciates CSA's clarification in Paragraph 4b that in-house penetration testing and managed SOC monitoring services, as well as companies that provide such services to their affiliated companies will be exempted from the licensing requirement. This is in line with the industry feedback provided in August 2017 and with Section 24(3) of the Cyber Security Act. We note however that this policy intent is not clearly stated in Annex A, "Draft Conditions of Licence".

For avoidance of doubt, we propose editing the definition of "Service" under Annex A as follows:

> "Service" means the licensable cybersecurity service that the Licensee is licensed to provide under the Licence, and refers EITHER to **commercially provided i)** penetration testing service OR **ii)** managed security operations centre (SOC) monitoring service, as respectively defined in paragraph 2 of the Second Schedule of the Act;

Licensing Requirements for Third-Party Service Providers

Industry had previously raised concerns over the lack of clarity on whether the licensing framework would be applicable to foreign service providers. BSA notes CSA's clarification in Paragraph 7 that cybersecurity service providers (**CSPs**) of licensable cybersecurity services, regardless of whether they are companies or individuals, based locally or overseas, will need to be licensed.

Given the rapidly evolving and global nature of cybersecurity breaches, imposing licensing requirements on local or overseas third-party service providers before they are allowed to provide licensable services to the Singapore market may restrict the ability for locally based CSPs to choose a technically competent local or overseas third-party vendor that could respond in a timely manner to cybersecurity breaches. This may inadvertently hinder CSPs' efforts to be as responsive as possible in adjusting their services to meet their customers' cybersecurity needs.

Instead of requiring third-party service providers to be licensed, we recommend that in such business scenarios, the main hiring CSP (i.e. the prime contractor for the service being engaged by the customer in Singapore) should be required to obtain the license and to keep records of the services

provided by the third-party service provider, including the types of services, and names of staff, as per the proposed regulation 4 in the draft SL.

Provision of Information

Paragraph 4.1 of Annex A specifies the various conditions under which licensees are required to provide CSA with information concerning or relating to its cybersecurity service. The industry recognizes the importance of supporting CSA in its evaluation and review of licensees by providing the necessary information relevant to the evaluation process. Currently, the provision in Paragraph 4.1 (a) could potentially be too broad; instead we recommend that licensees provide relevant information upon request, as follows:

4.1 The Licensee shall assist CSA **by providing relevant information** in any investigation **pertaining to** ~~– into~~ –

(a) ~~any matter relating to or arising from~~ the Licensee's application for grant or renewal of the Licence;

(b) any breach or potential breach by the Licensee of the Act or any licence conditions imposed on the Licensee; or

(c) ~~any matter relating to~~ the Licensee's continued eligibility to be the holder of the Licence.

Schedule of Licensable Services

While BSA notes that the list of licensable services in the Second Schedule is not part of the consultation, we would like to reiterate our position made in the previous submission that there should be a public consultation before any amendments are made. Any such consultation 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, with a grace period granted for compliance.

Conclusion

BSA is grateful for the opportunity to provide these comments and recommendations on the proposed draft licensing framework and SL to CSA. We support the Government of Singapore's efforts in implementing the Cybersecurity Act successfully and look forward to continuing to work with CSA on regulations and policies that will enhance cybersecurity. Please do not hesitate to contact the undersigned at eunicel@bsa.org if you have any questions or comments regarding our suggestions.

Yours faithfully,

Eunice Lim

Eunice Lim
Senior Manager, Policy – APAC
BSA | The Software Alliance