Technology, Media & Telecommunications

Industry Consultation on the Licensing Framework for Cybersecurity Service Providers

Introduction

The Cybersecurity Agency of Singapore ("**CSA**") has released its Industry Consultation Paper on the Licensing Framework for Cybersecurity Service Providers ("**CSPs**") under Part 5 of the Cybersecurity Act. While the rest of the Cybersecurity Act came into effect on 31 August 2018, the CSA intended for the licensing framework for CSPs to commence later after industry views on the implementation details have been gathered to enhance the practicality of the licensing framework.

The CSA has considered the feedback received on the proposed licensing framework during the public consultation on the Cybersecurity Bill held in 2017 in its drafting of Part 5 of the Cybersecurity Act. The current Industry Consultation is focused on the implementation details of the licensing framework. In this Update, we provide a background of the types and scope of licensable services and highlight the key proposed conditions of the licensing regime found in the Industry Consultation Paper.

Types of Licensable Services

The licensing regime would only apply to providers of managed security operations centre ("**SOC**") monitoring services and penetration testing services. The CSA decided to license these services as providers of these services would have access to sensitive information from their clients and there could be significant impact if services were not delivered well or misused. These services are also relatively mainstream in our market and hence have a significant impact on the overall security landscape.

Scope of Licensable Services

The CSA clarified that the licensing requirements will apply to all providers of the licensable service, regardless of whether they are companies or individuals (i.e., freelancers or sole proprietorships owned and controlled by individuals) who are directly engaged for such services, or third-party vendors that support these companies. Resellers, or overseas CSPs who provide licensable cybersecurity services to the Singapore market, would likewise need to be licensed.

The CSA also reiterated in its Industry Consultation Paper that companies providing penetration testing and managed SOC monitoring services in-house as well as companies that provide such services to their affiliated companies would not require a licence. The licensing regime would also not apply to individual cybersecurity professionals working under the employment of CSPs.

Key Proposed Conditions of the Licensing Regime

Information required for application of licence

To obtain a licence, information on the applicant's name, unique identification number and contact information must be provided along with information relating to the qualification or experience of the applicant (for individuals) or key officers (for business entities) relating to the licensable cybersecurity service for which a licence is sought. Where such information is not available, the applicant's employees having supervisory responsibility relating to the licensable service can be provided as an alternative. Information on whether the applicant is fit and proper must also be provided.

Keeping of records

Licensed CSPs are also required to keep records of the name and address of the person engaging the licensee for the service, along with the date and type of service provided. The licensee is also required to collect the name and individually identifiable information of the person providing the service on behalf of the licensee. For individuals, this would be the name and the unique identification number of the individual; for companies, this would be the business entity's name and unique entity number. Such records must be kept for a duration of at least three years. Licensees must ensure that these records are sufficiently detailed and complete, to allow for accountability and traceability in the event of foul play.

Notification on changes to information

To ensure that the licensees' key officers are fit and proper, licensees are to notify the licensing officer at least 30 days before the appointment of new key officer(s). Licensees must also notify the licensing officer of any change or inaccuracy of the information and particulars that the licensee had previously submitted within 14 days upon occurrence of the event. Such events include situations such as key officers ceasing to hold office, changes to the licensee's and/or its key officer's address and contact particulars, or criminal convictions entered against the licensee and/or its key officers.

Professional conduct of licensee

To provide a baseline level of protection for consumers of cybersecurity services, licensees would be required to comply with certain requirements on professional conduct such as the following:

(a) not make any false representation in the course of advertising or providing its cybersecurity service;
(b) comply with all applicable laws in the course of providing its cybersecurity service, including, but not limited to, the Computer Misuse Act (Cap. 50A) and all obligations relating to confidentiality and data protection;
(c) exercise due care and skill, and act with honesty and integrity in the course of providing its cybersecurity service;

(d) not act in a manner where there is a conflict between its interests and that of the person procuring or receiving the cybersecurity service; and
(e) collect, use, or disclose any information about (i) a computer or computer system of any person, or (ii) the business, commercial or official affairs of any person, only for the purposes of providing its cybersecurity service to the persons to whom the information relates.

Provision of information to the licensing officer

Licensed CSPs are also required to provide information concerning or relating to its cybersecurity service upon request and within stipulated timeframes to assist the CSA's investigation into:

(a) any matter relating to or arising from the licensee's application for grant or renewal of its licence;
(b) any breach or potential breach by the licensee of the Cybersecurity Act or any licence conditions; or
(c) any matter relating to the licensee's continued eligibility to be a holder of the licence.

Licence period and licence fees

The licence would be valid for two years and is renewable two months prior to expiry. The licence fees would be S$1,000 for business entities and S$500 for individuals. No application fees will be imposed on CSPs for the grant or renewal of licences. Due to the COVID-19 pandemic and its negative impact on businesses, 50% of the abovementioned fees will be waived for all applications lodged within the first 12 months from the commencement of the licensing framework (i.e., S$500 for business entities and S$250 for individuals). Existing CSPs will be given a six-month grace period to apply for the licence.

Concluding Remarks

The introduction of a licensing framework for cybersecurity service providers is generally to be welcomed for consumers as it provides a common and independent yardstick to assess if a cybersecurity service provider is legitimate and adheres to minimum industry standards. It also imposes minimum regulatory obligations and safeguards to be enforced by the CSA on cybersecurity service providers, beyond the available recourse against negligent service providers that consumers currently have under their contract terms. It is anticipated that the licensing regime will raise the level of professionalism amongst cybersecurity providers, similar to what has been observed in other industry sectors such as the real estate sector. This may attract more aspiring professionals to join the cybersecurity service sector to overcome the existing shortage.

However, as a matter of implementation, the licensing framework for cybersecurity service providers would have far reaching consequences for entities in the busines of providing licensable services. A failure to obtain a licence constitutes a criminal offence with a fine up to S$50,000 and/or imprisonment for a term up to two years. All affected persons or entities are therefore encouraged to carefully review the proposed licensing framework to ensure that any uncertainties in the scope of licensable services,

or practical difficulties in obtaining a licence or complying with licence conditions, are flagged out for CSA's clarification and consideration. Potential licensees should also start preparing for compliance with the licensing framework by considering the proposed licensing requirements and the steps that would need to be taken by your business to comply, as the licensing framework is expected to be come into effect shortly after its finalisation following the Industry Consultation.

The Industry Consultation will be held from 20 September 2021 to 18 October 2021 and all submissions should be provided to CSA no later than **5pm on 18 October 2021**. Should you have any queries on the above or require our assistance to submit a response to the Industry Consultation, please do not hesitate to get in touch with our team set out below.

Contacts

Rajah & Tann Singapore LLP

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0751
rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0786
steve.tan@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0752
lionel.tan@rajahtann.com

Benjamin Cheong
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0738
benjamin.cheong@rajahtann.com

Tanya Tang
Partner (Chief Economic and Policy Advisor), Competition & Antitrust and Trade; Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0298
tanya.tang@rajahtann.com

Rajah & Tann Technologies

Michael Lew
Chief Executive Officer, Rajah & Tann Technologies

T +65 6932 2609
michael.lew@rttechlaw.com

Rajah & Tann Cybersecurity

Wong Onn Chee
Chief Executive Officer, Rajah & Tann Cybersecurity

T +65 6932 2606
onnchee@rtcybersec.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

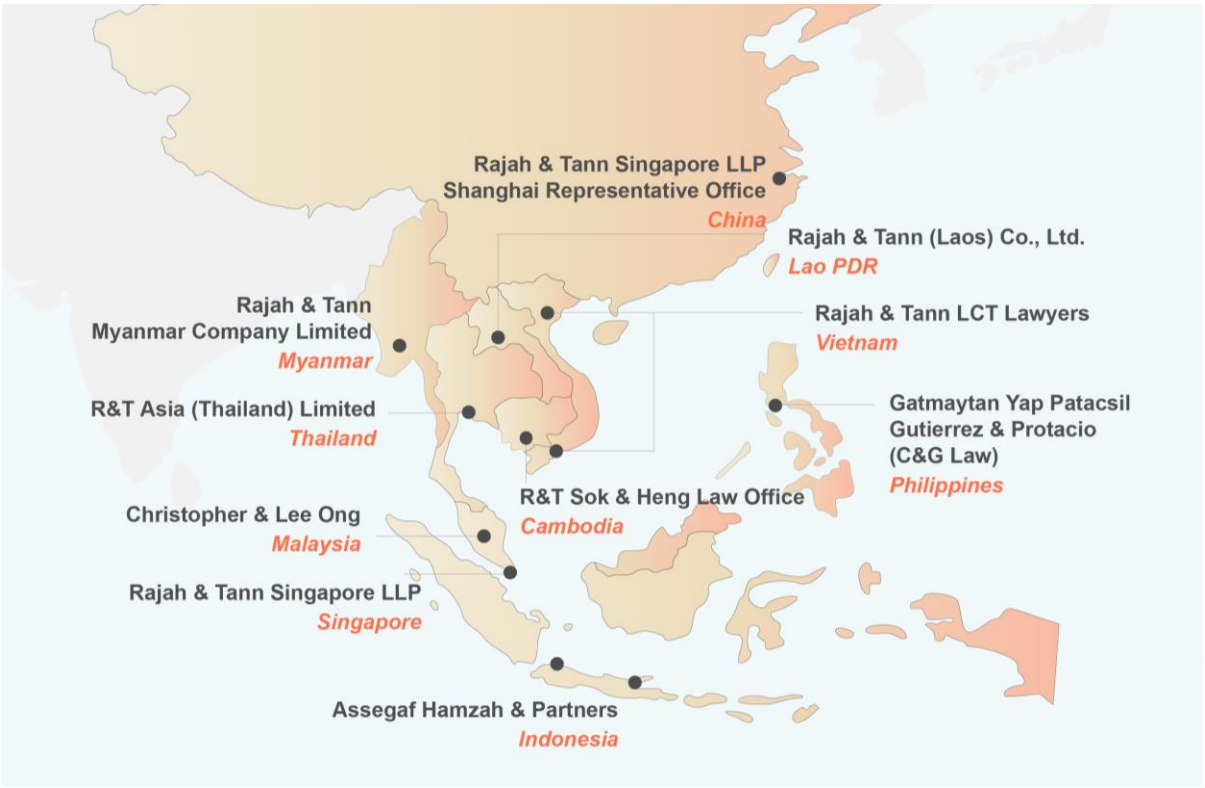
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.