Legislation

Industry Consultation on the Licensing Framework for Cybersecurity Service Providers

11 April 2022

Closing Note to Industry Consultation on the Licensing Framework for Cybersecurity Service Providers

11 April 2022

1. The Cyber Security Agency of Singapore ("CSA") held an industry consultation exercise on the proposed licence conditions and draft subsidiary legislation under the licensing framework for cybersecurity service providers found in Part 5 of the Cybersecurity Act (the "Act") from 20 September 2021 to 18 October 2021. The licensing framework aims to address three main considerations over time:

    a. Provide greater assurance of security and safety to consumers;

    b. Improve the standards and standing of cybersecurity service providers; and

    c. Address the information asymmetry between consumers and cybersecurity service providers.

2. CSA received a total of 29 responses at the close of the consultation, from a mix of local and foreign cybersecurity industry players, industry associations, and members of the public. The list of respondents is at Annex A [PDF, 87 KB] ↗.

Overview of Feedback Received

3. Overall, respondents were generally supportive of the licensing framework which will better safeguard consumers' interests while seeking to advance the industry's quality over time. Nonetheless, there were some respondents who expressed concerns of licensing stifling innovation or creating a regulatory burden on licensees.

4. CSA has taken into account and given thorough consideration to the respondents' feedback. This closing note seeks to address the key revisions to the licensing framework arising from the respondents' feedback, as well as feedback that are of wider interest to industry. For feedback that are more specific or clarificatory in nature, CSA may separately engage the respective respondents to provide the necessary clarification.

Responses to Feedback in Specific Areas

Proposed licence conditions

(i) Provision of information

5. Recap. To facilitate CSA's investigations into matters such as breaches by licensees or matters relating to the licensees' continued eligibility to be a holder of the licence, CSA proposed for licensees to provide the licensing officer with information concerning such matters that relate to their cybersecurity service upon request.

6. Feedback received. Some respondents suggested tightening the language of the proposed licence conditions to avoid requests that are overly broad. Some also requested more clarity on the types of information that might be requested.

7. CSA's response. CSA acknowledges the concerns raised and has revised the language of the licence conditions to reduce uncertainty for licensees. CSA would also like to indicate that any such information requested would be limited to what is necessary for the purpose of the investigation.

(ii) Notification on changes to information

8. Recap. To ensure that the licensees' key officers are fit and proper, CSA proposed for licensees to notify the licensing officer at least 30 days before the appointment of any new key officer. Licensees are also required to notify the licensing officer of any change or inaccuracy in the information and particulars that the licensee and/or its key officers have submitted to the licensing officer in relation to its licence within 14 days.

9. Feedback received. Some respondents highlighted that it may be impractical to require licensees to inform the licensing officer 30 days prior to the appointment of any new key officer due to legal or confidentiality constraints. Since the requirement was to inform the licensing officer rather than to seek approval for the appointment, some respondents suggested that licensees only inform the licensing officer after the key officer's appointment.

10. CSA's response. CSA has reviewed the feedback and will require licensees to inform the licensing officer of the appointment of any new key officer within 14 days after the key officer's date of appointment. This is aligned with the timeline for the other notification requirements as stated at paragraph 8. Licensees are reminded to ensure that any new key officer who is appointed must be fit and proper as defined in section 26(8) of the Act, failing which may result in punitive measures being imposed on the licensee, including revocation or suspension of licence.

(iii) Professional conduct of licensee

11. Recap. To provide a baseline level of protection for consumers of cybersecurity services, CSA proposed for licensees to comply with requirements such as maintaining confidentiality about their clients' information; not making any false representation in advertising their services or in the provision of its service; exercising due care and skill; and acting with honesty and integrity.

12. Feedback received. Some respondents sought clarifications on the licence condition relating to safeguarding of client information and cited concerns that it may potentially impact security research or responsible vulnerability disclosure. For instance, some respondents highlighted that cybersecurity service providers may aggregate or use anonymised data that is gathered from their engagements with clients for threat intelligence purposes. Another respondent shared that it may undertake responsible vulnerability disclosure in the event that critical vulnerabilities are found in the software, hardware, or firmware applications of its client's vendor, and if the said vendor had been unresponsive in resolving the cybersecurity vulnerabilities. The respondents were unclear whether such scenarios would constitute a breach of the licence condition.

13. CSA's response. Having considered the feedback, CSA has revised the specific licence condition by limiting its scope to the collection, use, and disclosure of information relating to the person procuring or receiving the licensable cybersecurity service. The use of anonymised information that is within the scope of this condition should be a matter to be agreed upon between the licensee and its

client. This condition is not expected to have any impact on responsible vulnerability disclosure processes.

(iv) Licence period

14. Feedback received. Some respondents suggested for the licence period to be lengthened from the proposed period of two years. Respondents also sought clarification on whether their existing licence will still be valid should licensees make their renewal applications two months prior to the licence expiry – which is in line with CSA's requirements – and if an outcome had yet to be reached by CSA prior to licence expiry.

15. CSA's response. Licence renewals serve as an important mechanism for CSA to make periodic assessments on whether licensees continue to remain fit and proper, which is fundamental to the safeguarding of consumers' interests. To strike a balance between security concerns and the minimising of administrative burden to cybersecurity service providers, CSA will proceed with the proposed licence period of two years for both licences as a start. This may be adjusted in future, subject to CSA's assessment on the cybersecurity service providers' level of compliance with the regulatory requirements. With regard to licence renewals, CSA would like to clarify that section 26(6) of the Act states that in the case of licensees who submit a renewal application before the start of the renewal period, the licence will continue to be in force until the date on which an outcome on the renewal application has been reached.

Draft subsidiary legislation

(i) Keeping of records

16. Recap. Under section 29(1) of the Act, licensees are required to keep records on the licensable cybersecurity services that it has provided for a duration of at least three years. In addition to the requirements stated at section 29(1)(a)(i) to (iv), CSA proposed for licensees to also keep records on the unique identifiers of the person providing the service on behalf of the licensee (e.g. identity card number if the person is an individual, or unique entity number if the person is a business entity).

17. Feedback received. Some respondents sought clarification on the record keeping requirements, and shared difficulties in meeting the requirements if licensees were required to keep records that could map all employees providing services to particular clients on a given date, particularly for managed security operations centre ("SOC") monitoring services which may involve a large number of employees working in shifts to provide round-the-clock monitoring.

18. CSA's response. CSA notes the respondents' concerns as well as suggestions to improve the practicality of the record keeping requirement. As conveyed in the industry consultation document, CSA does not intend to be prescriptive in how service records are kept (for instance, they may be kept in the form of source documents that substantiate the service provision such as contracts signed with clients, or relevant documents issued to or received from clients). The record keeping requirement would apply from the start of each engagement (i.e. provision of licensable cybersecurity services), and the service records must be retained for no less than three years after the engagement ends.

19. To provide greater clarity to cybersecurity service providers on the record keeping requirements, the examples at Annex B [PDF, 81 KB] ↗ serve to illustrate the level of detail expected should licensees be requested to furnish its service records to the licensing officer pursuant to section 29(2) of the Act.

Licensing scope and imposing of quality requirements

20. Recap. Under section 24(1) of the Act, it is an offence for a cybersecurity service provider to engage in the business of providing a licensable cybersecurity service without a licence. For a start, CSA will license only two types of service providers,

namely those providing penetration testing and managed SOC monitoring services as specified in the Second Schedule of the Act. All cybersecurity service providers that provide either or both of these licensable cybersecurity services to the Singapore market, 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 cybersecurity service providers that provide these services in support of other cybersecurity service providers (e.g. sub-contractors who are in the business of providing licensable cybersecurity services but may not be directly engaged by or have any direct contact with the main-contractors' clients), will need to be licensed. Resellers, or overseas cybersecurity service providers who provide licensable cybersecurity services to the Singapore market would likewise need to be licensed.

21. In view of the need to strike a good balance between industry development and cybersecurity needs, CSA intended for the licensing framework to be light-touch when introduced, with no quality requirements imposed on licensees at the outset.

22. Feedback received. While the above two areas were not within the scope of the industry consultation, respondents provided a range of views on how the licensing scope could be adjusted, such as scoping it more tightly to include only cybersecurity service providers that provide services to clients directly and to exclude sub-contractors or resellers; or expanding it to include other relatively more mature cybersecurity services. Some respondents raised the scenario of a cybersecurity service provider partnering with or leveraging the resources of an affiliate entity from its corporate group (which may be local or overseas) to provide licensable cybersecurity services. They suggested that for such arrangements that may involve different network business entities, only one entity within the corporate group should be required to obtain a licence. Some respondents also requested that CSA consult the industry or provide more clarity on the services that may be specified as licensable cybersecurity services in future, so that industry can prepare for any new obligations.

23. With regard to the imposing of quality requirements, some respondents provided suggestions on the requirements that CSA could consider, such as requiring licensees to be accredited, or for minimum training requirements to be imposed on staff of licensees.

24. CSA's response. CSA understands the concerns of possible administrative burden in scenarios where multiple entities involved in the provision of licensable cybersecurity services to the same client(s) are each required to take up a licence. However, regardless of the type of business partnership, consortium, or other legal arrangement entered into, the regulatory objective remains the same, which is to ensure that all persons (as elaborated at paragraph 20) engaging in the business of providing any licensable cybersecurity service to the Singapore market are fit and proper and meet the requirements of the Act, for the benefit and protection of consumers. Requiring only one entity to be licensed and introducing exemptions for the other entities (e.g. other entities within the same corporate group which are also in the business of providing licensable cybersecurity services), as some respondents had suggested, may undermine the aforementioned regulatory objective, especially since such business partnerships, consortiums, or legal arrangements may not be transparent to the clients.

25. As such, so long as any such entities engage in the business of providing any licensable cybersecurity service to the Singapore market (i.e. as per what is elaborated at paragraph 20), they must be licensed. Entities that assist in ways that do not constitute the provision of a licensable cybersecurity service (e.g. service providers who are involved in the mere provision of cybersecurity programs or tools intended to be installed by the users without further assistance from the service providers); entities that provide services other than for reward in the course of business; and entities that provide services to a related company for the latter's own benefit, are not required to be licensed.

26. Regarding the cybersecurity services that CSA may consider licensing in future, CSA will continue to monitor international and industry trends and engage the industry where necessary, as so to assess if any new types of cybersecurity services should be included in the licensing framework.

27. While CSA notes the healthy feedback from some respondents on the imposing of quality requirements, there were also respondents supporting the framework's light-touch approach. On balance, CSA will proceed with its intention not to impose any quality requirements at the outset but will continue to watch developments in this space. CSA will take the respondents' feedback into consideration should any quality requirements be introduced in the future.

Feedback on other areas

(i) Fit and proper requirements

28. Feedback received and CSA's response. Some respondents suggested that mental disorders be excluded from the fit and proper assessment of the key officers or individuals, given that some disorders could be minor and not relevant to the licence application. CSA will assess every key officer or individual on a case-by-case basis with the information they will be required to submit as part of the application for grant or renewal of licence. For each criterion, CSA would take into account the information shared and assess the degree to which it might affect the key officer's or individual's ability to perform his/her duty. For instance, in assessing applicants with previous criminal convictions, the licensing officer would also take into consideration factors such as seriousness and nature of the offence, and the time that has elapsed since the conviction. On the aspect of mental health, the primary consideration is that the key officer or individual should be mentally fit at the point of licence application and while his/her business entity or the individual remains a licensee. If the key officer's or individual's mental health condition is properly managed and certified by a qualified physician or healthcare professional, the presence of a mental health condition will not affect his/her or his/her business entity's eligibility to be licensed.

(ii) Definition of penetration testing service

29. Feedback received and CSA's response. Some respondents suggested for penetration testing service to be defined, given the potential confusion with vulnerability assessment. Some also sought clarification on whether individuals or business entities providing vulnerability assessment or red teaming services would also require a licence. CSA notes the feedback and would like to highlight that the definitions of penetration testing service and managed SOC monitoring service are already included in the Second Schedule of the Act.

30. Vulnerability assessments, which is commonly understood to involve the performance of scans on a client's IT systems or network to identify flaws that may be exploited during an attack, does not involve the compromise of the client's cybersecurity defences. This serves as a common distinction between vulnerability assessment and penetration testing, for which the former is not a licensable cybersecurity service.

31. Comparatively, red teaming, which is commonly understood to involve the simulation of a potential adversary's attack or exploitation capabilities, seeks to compromise the client's cybersecurity defences to demonstrate the impact of successful attacks. Red teaming involves the cybersecurity service provider utilising a range of techniques during the engagement, which may include penetration testing. cybersecurity service providers who provide red teaming services should also be licensed so long as their service would involve the performance of penetration testing (as defined in the Second Schedule).

(iii) Register of licensees

32. Feedback received and CSA's response. Some respondents suggested that a register of licensees be published for consumers to verify if their cybersecurity service providers are licensed. It is indeed CSA's intent to publish a list of licensees online, through which consumers could be encouraged to procure licensable cybersecurity services from cybersecurity service providers who are licensed. Nonetheless, consumers should also note that the published list only contains licensees providing penetration testing and/or managed SOC monitoring services. Consumers should consider their business needs and organisational goals to procure the appropriate types of cybersecurity solutions.

Conclusion

33. CSA would like to thank all respondents for their feedback, which has allowed us to identify aspects of the licensing framework that needed to be clarified or refined to enhance its practicability for cybersecurity service providers.

[1] These include: (i) the name and address of the person engaging the licensee for the service; (ii) the name of the person providing the service on behalf of the licensee; (iii) the date on which the service is provided; and (iv) details of the type of service provided.

Industry Consultation on the Licensing Framework for Cybersecurity Service Providers

20 September 2021

The Cyber Security Agency of Singapore (CSA) is seeking industry feedback on the proposed licence conditions and draft subsidiary legislation under the licensing framework for cybersecurity service providers found in Part 5 of the Cybersecurity Act.

Introduction

2. The Cybersecurity Act came into force on 31 August 2018 with the exception of the licensing framework under Part 5, which was then deferred to allow for further study and consultation to enhance its practicability for cybersecurity service providers. The licensing framework aims to address three main considerations over time:

    a. Provide greater assurance of security and safety to consumers;

    b. Improve the standards and standing of cybersecurity service providers; and

    c. Address the information asymmetry between consumers and the cybersecurity service providers.

3. For a start, CSA will license only two types of service providers, namely those providing penetration testing and managed security operations centre monitoring services. These two services are prioritised because service providers performing such services can have significant access into their clients' computer systems and sensitive information. In the event that the service is abused, the client's operations could be disrupted. In addition, these services are already widely available and adopted in the market, and hence have the potential to cause significant impact on the overall cybersecurity landscape.

Scope of Consultation

4. CSA is inviting industry feedback on the proposed licence conditions and draft subsidiary legislation. Some of the key proposals include:

    a. Professional conduct of licensees: To provide a baseline level of protection for consumers of cybersecurity services, CSA is proposing for licensees to

comply with requirements such as maintaining confidentiality about their clients' information; not making any false representation in advertising their services or in the provision of its service; exercising due care and skill; and acting with honesty and integrity.

b. Provision of information: To facilitate CSA's investigations into potential breaches by licensees, or matters relating to the licensees' continued eligibility to be a holder of the licence, licensed cybersecurity service providers are to provide information concerning or relating to its cybersecurity services upon request, and within the timeframes specified by the Licensing Officer.

c. Notification requirements: Under the Cybersecurity Act, cybersecurity service providers are required to ensure that their key executive officers are fit and proper persons when applying for a licence. Licensees are also required to keep records on the cybersecurity services that have been provided to clients for a duration of at least three years. To ensure that licensees remain fit and proper, CSA is proposing for licensees to notify the Licensing Officer within 14 days on changes to information such as those relating to the honesty, integrity and financial soundness of the business and its key executive officers, which may affect the licensee's continued eligibility to be licensed. To ensure that the licensees' key executive officers are fit and proper, licensees are to notify the Licensing Officer at least 30 days before the appointment of new key executive officer(s).

Period of Consultation

5. The industry consultation will be held from 20 September to 18 October 2021.

Submission Format and Feedback channel

6. Respondents should organise their submissions as follows:

    - Cover page (including name of the organisation/respondent; contact details such as the contact number and email address; and description of the licensable cybersecurity services provided by the organisation/respondent);
    - Summary of feedback;
    - Comments; and
    - Conclusion.

Supporting materials may be enclosed as an annex to the submission.

7. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any feedback. Where feasible, please identify the specific paragraph, condition, or regulation of the named document which you are commenting on.

8. All submissions should reach CSA no later than **5pm on 18 October 2021**. Late submissions will not be considered. Submissions are to be in softcopy only (in Microsoft Word format). Please send your submissions to Consultation@csa.gov.sg ↗, with the subject header "Industry Consultation on the Licensing Framework for Cybersecurity Service Providers".

9. CSA reserves the right to make public all or parts of any written submission and to disclose the identity of the source. Respondents may request confidentiality treatment for any part of the submission that the respondents believe to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex. Respondents are also required to substantiate with reasons any request for confidential treatment. If CSA grants confidential treatment, it will consider, but will not publicly disclose, the information. If CSA rejects the request for confidential treatment, it will return the information to

the respondent, and will not consider this information as part of its review. As far as possible, respondents should limit any request for confidential treatment of information submitted. CSA will not accept any submission that requests confidential treatment of all, or a substantial part, of the submission.

Documents to Download

10. The industry consultation document can be downloaded below, within which the proposed licence conditions and draft subsidiary legislation are set out at Annex A and Annex B respectively.

    - Industry Consultation Document [PDF, 378 KB] ↗

↑ Back to top