Industry Consultation Paper on the Licensing Framework

for Cybersecurity Service Providers

Issued by the Cyber Security Agency of Singapore (CSA)

20 September 2021

Content

PART 1: INTRODUCTION

Background on the Licensing Framework

1. The establishment of a light-touch licensing framework for the cybersecurity service providers ("CSP") was first introduced as one of the four objectives[1] under the draft Cybersecurity Bill (the "Bill"), which sought to establish a legal framework for the oversight and maintenance of national cybersecurity in Singapore. As the Cyber Security Agency of Singapore ("CSA") continues to raise awareness and encourage adoption of cybersecurity solutions by our businesses, the licensing framework sought to address three main considerations:

(a) Improve assurance on security and safety: As cybersecurity risks become more widespread, the demand for credible cybersecurity services will continue to grow. Some cybersecurity services can be sensitive and intrusive as the CSPs performing these services can have significant access into their clients' computer systems and networks, thereby gaining a deep understanding of their clients' cybersecurity posture and vulnerabilities. Such services, if abused, can compromise and disrupt the client's operations even after the CSPs' job has been completed. It is hence important that CSPs who are providing such sensitive services are fit and proper persons to reduce the safety and security risk that CSPs can pose.

(b) Raise quality and improve standing of the CSPs: The risks of cybersecurity services being carried out by incompetent or substandard CSPs are multi-fold, as computer systems may become vulnerable or damaged, suffer loss of information, and even endanger other systems. In view of the need to strike a good balance between industry development and cybersecurity needs, CSA does not intend to impose quality requirements on the CSPs as part of the licensing framework at the outset. Nonetheless, it is envisaged that licensing could serve as the means through which the quality of CSPs could be raised over time in future, such as through the introduction of a code of ethics or certain baseline competency requirements.

(c) Address information asymmetry: The complexities of a technical and evolving area like cybersecurity can give rise to the problem of information asymmetry, as buyers may not have expert knowledge and may not know which CSPs are ethical or of good quality. This is especially true for smaller buyers who do not have in-house cybersecurity expertise, thereby leading to a situation where buyers do not end up with appropriate cybersecurity services from credible service providers for their risks and budget. One objective of the licensing framework is hence to help organizations identify credible service providers, and increase demand for such services.

[1] The other three objectives include: (i) To strengthen the protection of critical information infrastructure against cyber-attacks; (ii) To authorise CSA to prevent and respond to cybersecurity threats and incidents; and (iii) To establish a framework for sharing cybersecurity information.

Past Consultations and Feedback Received

2. The Ministry of Communications and Information ("MCI") and CSA commenced work on the Bill in late 2015, and had conducted several rounds of closed-door consultations with stakeholders such as regulators of critical sectors, potential owners of critical information infrastructure ("CII"), industry associations and cybersecurity professionals to understand the ground sentiments and concerns.

3. A 6-week long public consultation on the Bill was held from 10 July to 24 August 2017. At the close of the public consultation, MCI and CSA received 92 submissions. Respondents were generally supportive of the Bill, and acknowledged the importance of having a legislative framework to protect the CII, as well as to give MCI/CSA the legislative powers to act on cybersecurity incidents that impact the nation. Specifically on the proposed licensing framework, feedback received were more diverse, with some respondents expressing reservations given the concerns of the licensing requirements being too onerous for businesses, and some requesting that the framework be simplified or made voluntary.

Response to Public Consultation (on the Proposed Licensing Framework)

4. The following provides a more in-depth summary of the feedback received on MCI/CSA's proposed licensing framework during the 2017 public consultation, and our corresponding responses that were published in the "Report on Public Consultation on the Draft Cybersecurity Bill" on 13 November 2017. MCI/CSA had then taken these feedback into consideration in the subsequent drafting of the Bill, which was passed on 5 February 2018 and received the President's assent on 2 March 2018 to become the Cybersecurity Act (the "Act")[2].

(a) Types of licensable services: The earlier proposed licensing framework made a distinction between "investigative" and "non-investigative" types of licensable services, in which penetration testing service providers would be licensed under an investigative cybersecurity service licence; while managed security operations centre ("SOC") monitoring service providers would be licensed under a non-investigative cybersecurity service licence. Some respondents suggested to reconsider the definitions of the two types of licensable cybersecurity services as they were too broad, and the proposed differentiation might become outdated as cybersecurity services evolve. In view of the feedback received to simplify the licensing framework, MCI/CSA did away with the distinction between "investigative" and "non-investigative" types of licensable services.

[2] Except for the provisions relating to the licensing of cybersecurity service providers, the rest of the Cybersecurity Act came into effect on 31 August 2018. Although the scope of services to be covered under CSA's licensing framework was determined earlier, CSA had intended for the licensing framework and this current industry consultation to commence later than the rest of the Act, to allow for further study and gathering of industry's views on the implementation details to enhance its practicability. The launch of this current consultation and related pre-consultation work were later deferred due to the COVID-19 pandemic, to provide affected cybersecurity service providers time and flexibility to focus on adjusting themselves to the challenging operating environment.

(b) Scope of licensing framework: Some respondents were against the licensing of CSPs as they felt that it could impact the development of a vibrant cybersecurity ecosystem in Singapore. In addition, there was feedback that it was unclear how the proposed licensing framework would treat the many other forms of cybersecurity service provision in the market, for instance resellers, and the provision of services by companies affiliated to the service buyers. Taking into consideration these feedback, MCI/CSA had scoped the licensing framework more narrowly, with only penetration testing and managed SOC monitoring service providers being licensed as a start, including resellers of such services, given that these services are already mainstream and widely adopted. In-house penetration testing and managed SOC monitoring services, as well as companies that provide such services to their affiliated companies are exempted.

(c) Licensing of cybersecurity professionals: Some respondents were concerned that the licensing of individual cybersecurity professionals (i.e. the individual penetration testers working under the employment of CSPs) would pose practical difficulties for global CSPs who deploy employees from their global centres around the world to deliver time-critical services. There were also suggestions on how the policy objectives for licensing could be achieved through alternative means such as accreditation of these professionals. In view of the feedback, MCI/CSA removed the requirement for individual cybersecurity professionals to be licensed. Consequently, CSPs would no longer be required to hire licensed cybersecurity professionals.

(d) Operational Costs on Businesses: MCI/CSA had also received feedback voicing concerns on how the licensing framework would impose an administrative burden on the CSPs, as the duration for which records of services provided must be kept was too long. Some also cautioned that the licensing framework should not impose onerous requirements on businesses. MCI/CSA had then clarified on its intent to keep the licensing fees low and requirements simple to minimise the operational costs on businesses. The licensing framework will be also be light-touch when introduced and akin to a registration regime. Lastly, the duration of service record keeping was reduced from the earlier proposed five years, to three years instead.

PART 2: RECAP ON SCOPE OF LICENSING FRAMEWORK

Main Licensing Requirements

5. To reiterate, MCI/CSA's licensing framework for the CSPs is intended to be light-touch when introduced and akin to a registration regime. As set out in Part 5 of the Act, the two main requirements that CSPs have to comply with include:

(a) Ensuring that their key officers are fit and proper: As defined in section 26(8), business entities are required to ensure that their key officers (i.e. any director or partner of the business entity or other person who is responsible for the management of the business entity) are fit and proper when applying for a licence. For instance, the key officer should not have had any criminal convictions or judgement entered against him/her in civil proceedings involving fraud, dishonesty or moral turpitude. Individuals applying for a CSP licence are also required to be fit and proper.

(b) Keeping of service records: As stipulated in section 29(1), licensed CSPs are required to keep basic records on the cybersecurity services that it has provided for a duration of at least three years. Examples of these records include: (i) name and address of the client engaging the licensed CSP for the cybersecurity service; and (ii) names of the persons providing the cybersecurity service on behalf of the licensed CSP.

Types of CSPs covered under the Licensing Framework

6. Under section 24(1), it is an offence for a CSP to engage in the business of providing a licensable cybersecurity service without a licence. As mentioned in paragraph 4(b), only two types of services are specified as licensable cybersecurity services as a start, which includes: (a) penetration testing service; and (b) managed SOC monitoring service.

7. All CSPs 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 CSPs that provide these services in support of other CSPs, will need to be licensed. Resellers, or overseas CSPs who provide licensable cybersecurity services to the Singapore market would likewise need to be licensed.

PART 3: PROPOSED LICENCE CONDITIONS AND SUBSIDARY LEGISLATION

Key Licence Conditions

8. Paragraphs 9 to 13 below serves to highlight some of the key proposed licence conditions (a fuller set of these conditions is set out at **Annex A**). The proposed licence conditions are applicable to both the Penetration Testing Service Licence and the Managed SOC Monitoring Service Licence.

Licence Period

9. As mentioned in paragraph 1(a), the licensing framework seeks to improve assurance on security and safety to consumers of cybersecurity services. To strike a balance between security concerns and the minimizing of administrative burden to CSPs, the licence period for both licences will be set at two years, and this is applicable to both new and renewed licences. The licence period may be adjusted in future, subject to CSA's assessment on the CSPs' level of compliance with the regulatory requirements.

Professional Conduct of Licensee

10. To provide a baseline level of protection for consumers of cybersecurity services, and to uphold the CSPs' professionalism, licensees will be required to comply with the following requirements on professional conduct:

(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. Licensees shall not collect, use or disclose any such information for other purposes, unless appropriate written consent has been obtained from the person to whom the information relates, or such collection, use, or disclosure is lawfully required by any court, or lawfully required or allowed under law.

Provision of Information

11. Licensed CSPs are to provide information concerning or relating to its cybersecurity service upon request, and within the timeframes specified by the licensing officer. These information are meant to assist CSA in its 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 Act or any licence conditions imposed on the licensee; or

(c) Any matter relating to the licensee's continued eligibility to be a holder of the licence.

Notification on Changes to Information

12. 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).

13. 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. These information and particulars may include, but are not limited to:

(a) When any key officer ceases to hold such office;

(b) Changes to or inaccuracies in the licensee's and/or its key officers' names, designations, addresses and contact particulars;

(c) Criminal convictions or civil judgments entered against the licensee and/or its key officers for offences or proceedings involving fraud, dishonesty, breach of fiduciary duty, or moral turpitude, or any offences under the Act;

(d) Criminal convictions entered against the licensee and/or its key officers for offences which involve a finding that the licensee and/or its key officers had acted fraudulently or dishonestly; or

(e) Where the licensee and/or its key officers have been declared bankrupt or have gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction.

14. CSPs are encouraged to put in place appropriate recruitment policies and internal controls systems and procedures, to ensure that their key officers are fit and proper and conduct themselves appropriately.

Key Regulations in the Subsidiary Legislation ("SL")

15. Paragraphs 16 to 22 below serve to highlight some of the key proposed regulations (please refer to **Annex B** which sets out the draft SL in full). The proposed regulations are applicable to both the Penetration Testing Service Licence and the Managed SOC Monitoring Service Licence.

Application for grant or renewal of licence

16. All applications for the grant or renewal of licence are to include the following (non-exhaustive) list of information, which are necessary for the licensing officer to make a thorough assessment of the application:

(a) The applicant's name;

(b) The applicant's individually identifiable information (for e.g. identity card number for applicants who are individuals, or the Singapore unique entity number for applicants which are business entities);

(c) The applicant's address, contact telephone number and email address;

(d) Information relating to the qualification or experience of —
   (i) The applicant (for applicants who are individuals) or key officers (for applicants which are business entities) relating to the licensable cybersecurity service for which a licence is sought; or
   (ii) If (i) is not available, the applicant's employees having supervisory responsibility relating to the licensable cybersecurity service; and

(e) Information relevant for the licensing officer to consider if the applicant is fit and proper (as stipulated in section 26(8) of the Act) (for applicants which are business entities, such information would also be required for every key officer).

Licence Fee

17. The licence is valid for two years and is renewable once every two years. The upfront two-year licence fees payable for both new and renewed licences will be S$1000 for business entities; and S$500 for individuals (i.e. freelancers or sole proprietorships owned and controlled by individuals). No application fees will be imposed on CSPs for the grant or renewal of licences.

18. Due to the COVID-19 pandemic which has negatively impacted many businesses, 50% of the abovementioned fees will be waived for all applications[3] lodged within the first 12 months from the commencement of the licensing framework. With the 50% fee waiver, the

[3] Existing cybersecurity service providers who are already in operations before the commencement of the licensing framework will be given six months from the commencement of the licensing framework to apply for a licence.

upfront payable licence fees for the two-year licence will be $500 for business entities and $250 individuals during the 12-month period.

Keeping of Records

19. As stated in paragraph 5(b), licensed CSPs are required to keep records on the licensable cybersecurity services that it has provided for a duration of at least three years. In accordance with section 29(1) of the Act and proposed regulation 4 in the draft SL, licensees are required to keep a record of the following information in relation to each occasion on which the licensee is engaged to provide its cybersecurity service:

(a) Name and address of the person engaging the licensee for the service;

(b) Name and individually identifiable information of the person providing the service on behalf of the licensee —
  (i) If the person is an individual, regardless whether or not the individual is an employee of the licensee, the following shall be kept —
    (A) The individual's name; and
    (B) The individual's identity card number, work pass number, passport number or foreign identification number;
  (ii) If the person is a business entity, the following shall be kept —
    (A) The business entity's name; and
    (B) The business entity's Singapore unique entity number, or business entity registration number in the foreign country or territory that the applicant is incorporated or registered in;

(c) Date on which the service is provided; and

(d) Details of the type of service provided.

20. While CSA does not intend to be prescriptive in the manner by which such service records are kept (for instance, in the form of a 24-hour duty roster or job sheet), licensees would need to ensure that these service records capture all the required information as stated above. These records should be sufficiently detailed and complete, to allow for accountability and traceability in the event of foul play.

Appeals

21. As stipulated in section 35, applicants or licensees may appeal to the Minister-in-charge of Cybersecurity against any of the following decisions made by the licensing officer:

(a) Refusal of an application for the grant or renewal of a licence;

(b) Addition or modification of conditions under section 27(3) during the grant or renewal of a licence;

(c) Revocation or suspension of a licence under section 30(1) and 30(2) respectively; or

(d) Order for the payment of a financial penalty under section 32(2) due to contravention of the Act or non-compliance with the licence conditions.

22. To prevent any incomplete submission and to allow for a smooth appeal process, the appeals are to be made via the form set out at https://www.mci.gov.sg, accompanied by all the relevant documents mentioned in, or relied on in support of the appeal. The appeal should also specify the name and particulars of the person bringing the appeal, identify the decision or order appealed against, and state the reasons for the appeal, amongst other details and/or requirements.

PART 4: INVITATION TO COMMENT

23. CSA would like to seek views and comments from the industry on the proposed licence conditions and subsidiary legislation in Part 3, which are set out in greater detail at **Annex A** and **Annex B**. Both the draft licence and the draft subsidiary legislation may be further refined, based on feedback received during this consultation.

24. All submissions should be clearly and concisely written. Where feasible, respondents should clearly identify the specific paragraph, condition, or regulation of the named document that they are commenting on in their submissions to CSA. Respondents may also propose changes to the proposed licence conditions and/or regulations in the SL. The proposals should be accompanied by reasons for these changes.

25. Submissions are to be in softcopy only (in Microsoft Word format), and should be organised as follows:

(a) 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);

(b) Summary of feedback;

(c) Comments; and

(d) Conclusion.

26. Supporting materials may be enclosed as an annex to the submission. Please email your submissions to Consultation@csa.gov.sg, with the subject header "*Industry Consultation on the Licensing Framework for Cybersecurity Service Providers*".

27. All submissions must reach CSA by **5pm on 18 October 2021**. Late submissions will not be considered.

28. 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.

Annex A

DRAFT CONDITIONS OF LICENCE

The following conditions are imposed under section 27 of the Cybersecurity Act 2018 (No. 9 of 2018) (the "**Act**") as conditions for the grant of a licence to provide licensable cybersecurity services. The conditions apply in addition to any requirements under the Act and the Cybersecurity (Cybersecurity Service Providers) Regulations 2021.

1. Definitions and interpretation

1.1. In these conditions, unless the context otherwise requires:

"Officer" refers to "officer of a business entity" as defined in section 26(10) of the Act, namely, any director or partner of the business entity or other person who is responsible for the management of the business entity.

"Licence" means the licence granted or renewed by the Licensing Officer to the Licensee to provide the relevant Service as stated therein;

"Licensee" means the holder of a Licence;

"Licensing Officer" means the Commissioner of Cybersecurity appointed under section 4(1)(a) of the Act;

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

1.2. Apart from the definitions in paragraph 1.1 above, any other word or expression used in these conditions shall have the same meaning as in the Act unless the context otherwise requires.

1.3. This Licence is subject to the provisions of the Act and of any law amending, modifying or replacing the same. Any reference to the Act shall include any subsidiary legislation, rules, regulations and directions or orders made pursuant thereto.

1.4. For the avoidance of doubt, the Licensee shall comply with all obligations under the Act and this Licence at its own costs, unless otherwise specified in writing by the Licensing Officer.

2. Licence Period

2.1. The Licence is valid for two years, unless revoked or suspended by the Licensing Officer in accordance with section 30 of the Act.

2.2. Any application to renew the licence shall be made in accordance with the requirements and timelines prescribed in the Act.

2.3. Where an application to renew the licence is made after the time prescribed by the Act, the application will be treated as a fresh application for grant of a licence.

3. Professional Conduct of Licensee

3.1. In relation to the Service it provides, the Licensee shall:

(a) Not make any false representation in the course of advertising or providing the Service;

(b) Comply with all applicable laws in the course of providing the 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 the Service;

(d) Not act in a manner where there is a conflict between its interests and that of the person procuring or receiving the 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 the Service to the persons to whom the information relates. The Licensee shall not collect, use or disclose any such information for other purposes, unless appropriate written consent has been obtained from the person to whom the information relates, or such collection, use, or disclosure is lawfully required by any court, or lawfully required or allowed under law;

3.2. The Licensee shall also take all reasonable steps in the circumstances to ensure that its Officers, employees and/ or contractors also comply with the matters listed in paragraphs 3.1(a) to (e) above, with all references to the Licensee to be read as references to such persons.

4. Provision of Information

4.1. The Licensee shall assist CSA in any investigation 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.

4.2. The Licensee shall produce, at its own expense and within the timeframes specified by CSA, any such information, records, documents, data or other materials as may be required by CSA for the purposes of any investigation under this paragraph 4 (referred to collectively in this paragraph as the "Relevant Information").

4.3. The Licensee shall keep confidential any information relating to such investigations, including but not limited to the fact that investigations are being conducted, or details regarding any Relevant Information provided by the Licensee to CSA. All reasonable care must be taken to safeguard the confidentiality of the information, and Licensees shall not communicate the information to any person without prior written consent from CSA. For the avoidance of doubt, CSA can at any time determine that certain categories of information need no longer be treated as confidential.

5. Changes to Information

5.1. The Licensee shall notify the Licensing Officer, in the manner described in CSA's website at https://www.csa.gov.sg of any change or inaccuracy in the information and particulars that the Licensee and/or its Officers submitted to the Licensing Officer in relation to this Licence, within fourteen (14) calendar days of such change or knowing of such inaccuracy (exclusive of the day such change or knowledge occurs). Such information and particulars include, but are not limited to:

(a) When an Officer ceases to hold such office;

(b) Changes to or inaccuracies in the Licensee's and/or its Officers' names, designations, addresses and contact particulars;

(c) Criminal convictions or civil judgments entered against the Licensee and/or its Officers for offences or proceedings involving fraud, dishonesty, breach of fiduciary duty, or moral turpitude, or any offences under the Cybersecurity Act 2018;

(d) Criminal convictions entered against the Licensee and/or its Officers for offences which involve a finding that the Licensee and/or its Officers had acted fraudulently or dishonestly; or

(e) Where the Licensee and/or its Officers have been declared bankrupt or have gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction.

5.2. Notwithstanding paragraph 5.1 above, the Licensee shall, at least 30 calendar days before the effective date of appointment of any Officer (exclusive of the day such appointment occurs), notify the Licensing Officer of any such appointment and complete the forms set out for this purpose at *GoBusiness Licensing* at https://www.gobusiness.gov.sg/licences.

6. Other Licences

6.1. Nothing in this Licence affects the requirement to obtain any other licence that may be required under the Act or any other written law.

7. Use of symbol or logo

7.1. The Licensee shall not do any of the following in relation to any symbol or logo that CSA uses in connection with its activities or affairs, except with prior written permission of the Licensing Officer:

(a) Use any symbol or logo that is identical with those used by CSA; and

(b) Use any symbol or logo that is similar to those of CSA in a manner that is likely to deceive or cause confusion.

DRAFT CYBERSECURITY (CYBERSECURITY SERVICE PROVIDERS) REGULATIONS 2021

ARRANGEMENT OF REGULATIONS

Regulation

Citation and commencement

1. These Regulations are the Cybersecurity (Cybersecurity Service Providers) Regulations 2021 and come into operation on [date].

Applications for grant or renewal of licence

2.—(1) Subject to paragraph (4), every application for the grant or renewal of a licence must be made electronically using the electronic application service provided by the licensing officer at https://www.gobusiness.gov.sg/licences.

(2) The application for the grant or renewal of a licence must include the following:

(*a*) where the applicant is an individual —

(i) the applicant's name;

(ii) the applicant's identity card number, work pass number, passport number or foreign identification number;

(iii) the applicant's nationality;

(iv) the applicant's residential address and, if different, the applicant's correspondence address;

(v) the applicant's contact telephone number and email address;

(vi) information relating to —

(A) the applicant's qualification or experience (if any) relating to the licensable cybersecurity service for which a licence is sought;

(B) where the applicant does not have any qualification or experience relating to the licensable cybersecurity service for which a licence is sought — the qualification or experience of the applicant's

employees or proposed employees having supervisory responsibility relating to the licensable cybersecurity service; or

(C) where sub-paragraphs (A) and (B) are not applicable — the business partnership, consortium or other legal arrangement (if any) through which the applicant proposes to provide the licensable cybersecurity service;

(vii) information as to whether the applicant has been convicted in Singapore or elsewhere of —

(A) an offence involving fraud, dishonesty or moral turpitude; or

(B) an offence the conviction for which involves a finding that the applicant had acted fraudulently or dishonestly;

(viii) information as to whether the applicant has had a judgment entered against the applicant in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the applicant;

(ix) information as to whether the applicant is or was suffering from a mental disorder;

(x) information as to whether the applicant is an undischarged bankrupt or has entered into a composition with any creditor of the applicant;

(xi) information as to whether the applicant has had a licence revoked by the licensing officer previously; and

(xii) any other information that may be specified by the licensing officer in the electronic application service mentioned in paragraph (1);

(*b*) where the applicant is a business entity —

(i) the applicant's name;

(ii) the applicant's —

(A) Singapore unique entity number; or

(B) business entity registration number in the foreign country or territory that the applicant is incorporated or registered in;

(iii) the address of the applicant's registered office or principal place of business;

(iv) if the address in sub-paragraph (iii) is outside Singapore, the address of the applicant's principal place of business or address for service in Singapore;

(v) the applicant's contact telephone number and email address;

(vi) the particulars mentioned in sub-paragraph (*a*) (except sub-paragraph (*a*)(vi)(B) and (C)) in respect of every director or partner of the applicant or other person who is responsible for the management of the applicant, with each reference in sub-paragraph (*a*) to the applicant substituted with a reference to the director, partner or other person, as the case may be;

(vii) where no director or partner of the applicant or other person who is responsible for the management of the applicant has any qualification or experience relating to the licensable cybersecurity service for which a licence is sought — information relating to the qualification or experience of the applicant's employees or proposed employees having supervisory responsibility relating to the licensable cybersecurity service for which a licence is sought;

(viii) information as to whether the applicant has been convicted in Singapore or elsewhere of —

(A) an offence involving fraud, dishonesty or moral turpitude; or

(B) an offence the conviction for which involves a finding that the applicant had acted fraudulently or dishonestly;

(ix) information as to whether the applicant has had a judgment entered against the applicant in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the applicant;

(x) information as to whether the applicant is in liquidation or is the subject of a winding up order, or there is a receiver appointed in relation to the applicant, or the applicant has entered into a composition or scheme of arrangement with any creditor of the applicant;

(xi) information as to whether the applicant has had a licence revoked by the licensing officer previously; and

(xii) any other information that may be specified by the licensing officer in the form set out at the electronic application service mentioned in paragraph (1).

(3) An application for the renewal of a licence must be made no later than 2 months before the date of expiry of the licence.

(4) If the electronic application service is not operating or available, an application for the grant or renewal of a licence must be made in such written form as the licensing officer may require.

(5) If an application for the renewal of a licence cannot be submitted in accordance with paragraph (1) within the time specified in paragraph (3) due to the unavailability of the electronic application service, an application in such written form mentioned in paragraph (4) must be submitted on the next working day to the licensing officer.

(6) In this regulation, "employee having supervisory responsibility relating to the licensable cybersecurity service", in relation to an applicant, means an employee of the applicant who is responsible for supervising or managing the provision of a licensable cybersecurity service or any part of a licensable cybersecurity service by any other employee of the applicant.

Licence fee

3.—(1) The fee payable for the grant or renewal of a licence is the following:

(*a*) where the applicant is an individual —

(i) $125 per year or part of a year, where the application is made to the licensing officer during the initial period; or

(ii) $250 per year or part of a year, where the application is made to the licensing officer after the expiry of the initial period;

(*b*) where the applicant is a business entity —

(i) $250 per year or part of a year, where the application is made to the licensing officer during the initial period; or

(ii) $500 per year or part of a year, where the application is made to the licensing officer after the expiry of the initial period.

(2) The licensing officer may, where the licensing officer considers appropriate, refund or remit the whole or part of any fee paid or payable under paragraph (1).

(3) In this regulation, "initial period" means the period beginning on [date of commencement of these Regulations] and ending on [the date immediately before the 12-month anniversary of the date of commencement of these Regulations] (both dates inclusive).

Keeping of records

4.—(1) For the purposes of section 29(1)(*a*)(v) of the Act, a licensee must, in relation to each occasion on which the licensee is engaged to provide its cybersecurity service, keep records of the information specified in paragraph (2) in respect of every person who delivers the cybersecurity service on behalf of the licensee.

(2) For the purposes of paragraph (1) —

(*a*) the information for which records must be kept in respect of every individual who delivers any part of the cybersecurity service on behalf of the licensee, whether or not the individual is an employee of the licensee, is the following:

(i) the individual's name;

(ii) the individual's identity card number, work pass number, passport number or foreign identification number;

(*b*) the information for which records must be kept in respect of every business entity which delivers any part of the cybersecurity service on behalf of the licensee is the following:

(i) the business entity's name;

(ii) the business entity's —

(A) Singapore unique entity number; or

(B) business entity registration number in the foreign country or territory that the applicant is incorporated or registered in.

Appeals

5. An appeal made under section 35(1), (2), (3) or (4) of the Act must —

(*a*) be made in the form set out at https://www.mci.gov.sg;

(*b*) specify the name and particulars of the person bringing the appeal (called in this regulation the appellant);

(*c*) identify the decision or order appealed against;

(*d*) state the reasons for the appeal and the issues arising from the appeal;

(*e*) be accompanied by any document mentioned in, or relied on in support of, the appeal; and

(*f*) be signed and dated —

(i) where the appellant is an individual — by that individual or a duly authorised representative of the individual; or

(ii) where the appellant is a business entity — by a duly authorised representative of the business entity.

Made on 2021.