



**RESPONSE TO INDUSTRY CONSULTATION ISSUED BY CYBER SECURITY AGENCY OF  
SINGAPORE**

---

**FEEDBACK ON THE LICENSING FRAMEWORK FOR CYBERSECURITY SERVICE  
PROVIDERS**

**FROM**

**THE AMERICAN CHAMBER OF COMMERCE, SINGAPORE**

**18 OCTOBER 2021**

*Contact:*

*Jessica Cho*

*Head, External Affairs*

*[jcho@amcham.com.sg](mailto:jcho@amcham.com.sg)*

*1 Scotts Road, #23-03/04/05*

*Shaw Centre Singapore 228208*

18 October 2021

Mr. Koh Tee Hian David  
Cyber Security Agency of Singapore  
5 Maxwell Road  
#03-00 Tower Block, MND Complex  
Singapore 069110

## **AMCHAM INPUT ON THE PROPOSED LICENSE CONDITIONS AND DRAFT SUBSIDIARY LEGISLATION UNDER THE LICENSING FRAMEWORK FOR CYBERSECURITY SERVICE PROVIDERS**

### **SUMMARY OF FEEDBACK**

The American Chamber of Commerce in Singapore (AmCham) welcomes the opportunity to provide input to the Cyber Security Agency of Singapore (CSA) for the proposed license conditions and draft subsidiary legislation under the licensing framework for cybersecurity providers.

AmCham is the largest and most active international business association in Singapore and Southeast Asia, with over 5,000 members representing nearly 550 companies. Many U.S. companies establish their regional headquarters in Singapore before scaling up and expanding in the region. Our goal is to meet present and future challenges to the mutual benefit of American business and the people of Singapore.

AmCham's feedback on the licensing framework for cybersecurity providers is centered on the following key proposals:

- I. Provision of Information
- II. Notification on Changes to Information
- III. Keeping of Records

### **COMMENTS**

#### **Provision of Information**

In regard to the provision for licensees to assist CSA in investigations, AmCham encourages CSA to clarify the standards that will be used to determine any "potential breach".

Under 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.

AmCham is concerned that the overly wide investigative powers as encapsulated in this provision increases uncertainty and subjectivity for licensees. AmCham recommends that CSA provide clear standards that will be used in determining what would constitute a potential breach.

### **Notification on Changes to Information**

AmCham strongly encourages CSA to consider removing the obligation for licensees to notify CSA before the appointment of new key officers due to potential legal and practical constraints in abiding with this clause.

Under 5.2, 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.

Given the pressing need for business efficiency in the field of penetration testing and monitoring services, particularly during a crisis, the 30-day requirement may not be practical or feasible for licensees. Further, employment contractual obligations often include confidentiality policies that would render this provision impractical for licensees to comply with.

### **Keeping of Records**

AmCham recommends CSA to reduce the scope in the keeping of records as this provision would be impractical for global teams to meet.

Under 19, licensees are required to keep records of the name and address of the person engaging the licensee for the service to the particular customer.

The nature of global managed security operations centre (SOC) monitoring service includes multiple teams across jurisdictions to provide round-the-clock monitoring. The large number of individuals involved in providing such services renders this provision both difficult and impractical for licensees. AmCham encourages CSA to consider reducing the scope of this provision, such that it may be sufficient to maintain proper records of all employees deployed to manage customers for any given period, rather than map each employee to specific customers.

### **CONCLUSION**

Singapore has a vibrant cybersecurity ecosystem, and its legislature should allow for continued growth of this leading industry sector. AmCham greatly appreciates the efforts of CSA in facilitating open discussions with industry to improve industry standards. We look forward to working closely together with the Government on advancing Singapore's cybersecurity strategy.

Yours Sincerely,



Dr. Hsien-Hsien Lei  
Chief Executive Officer