RESPONSE TO INDUSTRY CONSULTATION ISSUED BY CYBER SECURITY AGENCY OF SINGAPORE

FEEDBACK ON THE PROPOSED UPDATES FOR THE CYBERSECURITY CODE OF PRACTICE

FROM

THE AMERICAN CHAMBER OF COMMERCE IN SINGAPORE

13 MAY 2022

Contact:
Jessica Cho
Head, External Affairs
jcho@amcham.com.sg

1 Scotts Road, #23-03 Shaw Centre, Singapore 22820
Tel: (65) 6597 5730 | www.amcham.com.sg
Registration No. ROS 239/73 TAP

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

AMCHAM INPUT ON THE PROPOSED UPDATES TO THE CYBERSECURITY CODE OF PRACTICE

SUMMARY OF FEEDBACK

The American Chamber of Commerce in Singapore (AmCham) welcomes the opportunity to provide comments to the Cyber Security Agency of Singapore (CSA) on the draft Cybersecurity Code of Practice (CCoP).

AmCham is the largest and most active international business association in Singapore and Southeast Asia, with over 5,000 members representing over 550 companies with regional headquarters in Singapore. 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 updates to the Cybersecurity Code of Practice (CCoP) is centered on the following key areas:

I. Narrowing Down the Scope Of CIIO
II. Clarity on Timelines for Waivers
III. Clarity on Use of Cloud
IV. Clarity on Vendor Management and Remote Connection
V. Alignment with International Standards and Global Practices
VI. Promoting Free Flow of Data Across Borders

COMMENTS

Narrowing Down the Scope of CIIO

In regard to Section 1.4.1 under Scope and Applicability, AmCham encourages CSA to further define what kind of entity qualifies as a CII.

This is relevant in cases where the CIIO is leveraging third party vendors or possibly has entities with operations that are not directly connected with the CIIO operations. AmCham recommends that CSA further define the definition to specific entity/entities with operations that are impacted by the CCoP regulations.

Clarity on Timelines for Waivers

AmCham would appreciate clarity on the timelines for waiver applications.

Under Section 1.6 (Waiver):

1.6.1 The Commissioner may waive the application of any specific provisions of this Code to a CIIO under section 11(7) of the Act.

1.6.2 A CIIO shall request for waiver from specific provisions of this Code under section 11(7) of the Act by submitting a written request to the Commissioner with the justifications supporting the request.

AmCham notes that there is no indication of duration of the waiver process or the response timeline from CSA on waiver applications. Given the time sensitive nature of cyber operations, AmCham welcomes CSA to (i) clearly define the amount of time needed to hear back on a waiver request; and (ii) clarify if entities would still be required to adhere to the CCoP while the waiver request is being reviewed.

Clarity on Use of Cloud

Timeline

Under Section 3.7 (Use of Cloud):

3.7.2 The CIIO shall consult the Commissioner when planning to move the CII to the Cloud.

3.7.5 The CIIO shall conduct a cybersecurity risks assessment to ensure that the risks of the CII moving to the Cloud are adequately addressed. The completed cybersecurity risks assessment must be formally accepted by the CIIO and submitted to the Commissioner no later than 30 days after completion for review.

AmCham notes that the timeline for the consultation process with the Commissioner under Section 3.7.2 is unclear. Additionally, under Section 3.7.5, it is unclear when a CIIO will receive a response from CSA.

For Section 3.7, AmCham recommends CSA to clarify (i) the timeline of the risk assessment process; and (ii) what will the process look like. AmCham further recommends the language in Section 3.7.2 be changed from “consult” to “inform”, as a risk assessment process is already mandated in Section 3.7.5. A risk assessment process should be sufficient so there is no need for a consultation process as well.

Governance

Additionally, under Section 3.7 (Use of Cloud)

3.7.3 The CIIO shall ensure that CII assets in the Cloud are governed under Singapore laws and regulations.

3.7.4 The CIIO shall ensure that the third-party vendor providing cloud services is, or is affiliated to, a business entity that is registered in Singapore, or under an agreement governed by Singapore law.

AmCham notes that CSA has introduced Section 3.7.3, which provides that CII assets in the cloud must be governed under Singapore laws and regulations. However, the definition of "CII asset" under the CCoP is broad, and assets in an overseas data center are unlikely to be directly governed by Singapore law. This is in effect a data localization requirement.

AmCham recommends for Section 3.7.3 be removed as Section 3.7.4 (which requires that the CIIO ensure that the third-party cloud services vendor is, or is affiliated to, a business entity that is registered in Singapore, or under an agreement governed by Singapore law) is sufficient to ensure that there is a legislative and practical hold over the cloud service provider.

Clarity on Vendor Management and Remote Connection

3.8.1 (Vendor Management): The CIIO shall be responsible and accountable for the cybersecurity of its CII, even if it outsources any aspect of its CII activities.

While the intention is for the CIIO to be held responsible, much of the responsibility could be shifted towards vendors and CII through contractual obligations. AmCham recommends CSA to clarify to what extent CIIO can outsource its CII activities.

5.6.3 (Remote Connection): For remote connections to a CII, the CIIO shall adopt the following practices: (d) Implement encryption for remote connections.

For industries such as manufacturing, which may have difficulties with encryption, AmCham suggests that the CII implement appropriate security controls for remote connections based on its business requirements and to be tailored to different industries.

Alignment with International Standards and Global Best Practices

AmCham recommends aligning cybersecurity policies and approach with international standards and best practices. Businesses are facing an increasingly fragmented global regulatory landscape. Companies that want to invest and participate in the market often encounter legal challenges that lessen their ability to comply with multiple, overlapping, conflicting, and duplicative security measures. Cybersecurity requirements and notification obligations that are globally aligned minimize complexities, reduce administrative burdens, and improve systems security.

Where possible, cybersecurity policies should rely on existing standards such as the approaches embodied in the National Institute of Standards and Technology (NIST) Framework for

Improving Critical Infrastructure Cybersecurity (Framework) that were developed through an international multi-stakeholder process.

Promote free flow of data across borders

AmCham encourages CSA to consider adopting risk-based approaches that permit innovation and the free flow of data while meeting the legitimate security needs of law enforcement agencies.

Cyber incidents and risk management activities are international in scope and network monitoring, trends, and threat information are shared across borders. Information security professionals rely on timely access to cyber threat data (e.g., signatures, indicators of compromise, vulnerabilities) to enhance situational awareness, calibrate defensive measures, and share mitigation strategies with stakeholders. Restrictive localization regulations artificially create cyber risk by creating blind spots that inhibit timely and actionable information exchange.

CONCLUSION

Singapore has a vibrant and growing cybersecurity ecosystem. As such, 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 encourage CSA to continue conducting regular industry consultations that include vendors as well as CIIOs. 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