CYBERSECURITY ACT

FREQUENTLY ASKED QUESTIONS

Section I: Development of the Act

1. What was the consultation process for the development of the Act, and what was the general feedback received from the public consultation?

MCI and CSA commenced work on the Act in late 2015. Since then, MCI and CSA had conducted five rounds of closed-door consultations with key stakeholders, ranging from government agencies, potential critical information infrastructure (CII) owners, industry associations, and cybersecurity professionals. MCI and CSA held a public consultation on the draft Bill from 10 July to 24 August 2017, where the deadline was extended by 3 weeks, in response to public requests for more time to provide feedback. A total of 92 submissions were received during the public consultation process.

Respondents were generally supportive of the Bill and understood the importance of such a Bill to enhance the cybersecurity landscape in Singapore for the benefit of the people and businesses**.** They shared the Government's concerns on cyber threats and the impact of cyber-attacks on Singapore. They acknowledged the importance of the Bill in providing the necessary legislative framework to better protect CII, and to give CSA the legislative powers required to act on cybersecurity incidents that impact the nation. Several respondents also agreed with the importance of sharing cybersecurity information between CSA and other organisations, and the need to safeguard the sources and information disclosed.

However, several respondents expressed reservations with the proposed licensing framework. They felt that the requirements to be imposed on businesses should not be too onerous. Several suggested simplifying the licensing framework, or making it voluntary, e.g. through an accreditation regime.

The feedback provided has been taken into consideration in the drafting of the Bill.

2. Will there be further consultations on implementation details?

CSA will be engaging the industry further on implementation details such as the licensing requirements for cybersecurity service providers.

3. How does the Act compare against international examples, in terms of powers granted to the government?

Legislation in other countries generally accords authorities with powers in some of the following five areas:

(i) Standards setting,
(ii) Information sharing,
(iii) Incident management,
(iv) Crisis management, and
(v) International conduct.

The Act is not out of step with international developments, but will be one of the most comprehensive cybersecurity laws covering three of the five areas: standards setting, information sharing, and incident management. The Act does not provide for emergency/crisis powers, or international conduct (e.g. harmonisation with other countries' laws, or mandate for international engagement).

Notably, Singapore will be among the first countries in the world to regulate cybersecurity service providers, specifically penetration testers and managed security operations centre (SOC) monitoring service providers.

The licensing framework will be light-touch when introduced, in that licensed cybersecurity service providers will need to fulfil only basic requirements that are set out in Part 5 of the Act. For example, they have to ensure that their key executive officers and employees performing the licensable services are fit and proper persons, as well as keep service records for a duration of 3 years. Where licensable cybersecurity services are provided to related companies, the providers will not require a licence.

Beyond the Act, CSA will continue to work with the industry and professional association partners to establish voluntary accreditation regimes for cybersecurity professionals, to improve the standing of cybersecurity professionals. This will complement the light-touch licensing framework for cybersecurity service providers, which will not impose quality requirements as part of the licensing conditions at the outset.

4. Why is there a need for a new Cybersecurity Act?

There are no laws in Singapore today that directly ensures the routine protection of CII. Today, Section 15A of the Computer Misuse and Cybersecurity Act (CMCA) empowers the Minister for Home Affairs to issue a certificate to authorise or direct a person or an entity to take measures to comply with requirements necessary to prevent, detect or counter a threat to the national security, essential services, defence or foreign relations of Singapore if the Minister is satisfied that it is necessary for the purpose of preventing, detecting or countering any threat to the national security, essential services, defence or foreign relations of Singapore. However, the CMCA, which mainly deals with cybercrimes such as the unauthorised access of computer material, does not provide a regulatory framework for the routine and proactive protection of CII.

The Cybersecurity Act will enhance the powers available in Section 15A of the CMCA by providing more powers and which focus explicitly on cybersecurity. For instance, Section 15A allows the Government to request for information to protect against cybersecurity threats, but does not mandate CII incident reporting or facilitate the sharing of cybersecurity information with the Government. The Cybersecurity Act will address these gaps.

Today, CSA works with sector regulators to coordinate cybersecurity efforts to protect CII within their own sectors. The sectors have varying levels of cybersecurity readiness, and sector regulators have varying powers under their respective legislation and regulations to regulate CII within their sectors on cybersecurity matters.

While some Sector Leads have powers to regulate CII owners, such regulation tends to be outcome-based and was not designed with cybersecurity in mind. For example, rail operators and telcos are largely regulated based on their ability to meet service standards, not based on their compliance with cybersecurity requirements.

Other Sector Leads do not see themselves as regulators as their relationship with the CII are contractual, or they are CII owners themselves. These sectors are unlikely to have strong incentives to invest in cybersecurity of their own accord.

Section II: Administration of the Act

5. How will the Act empower Sector Leads?

The Act allows the Minister to appoint Assistant Commissioners (ACs) to assist the Commissioner to oversee and enforce cybersecurity requirements on the owners of CII, and the intention is to appoint officers from sector regulators as ACs to perform this role. This is because sector regulators understand the unique contexts and complexities in their sectors, and will be best-placed to advise on the necessary requirements so as to strike a balance between their sector's cybersecurity needs and operational considerations.

The Act will provide CSA and Assistant Commissioners appointed from Sector Leads, such as the Energy Market Authority (EMA) for the energy sector, with the necessary levers to proactively protect our CII and respond to cybersecurity threats and incidents.

However, it is recognised that not all Sector Leads may be ready to assume the cybersecurity regulatory role at the current moment. The Act provides for the flexibility for the Commissioner to assume direct oversight over certain CII.

6. What are the powers of the Assistant Commissioner?

The Assistant Commissioner has and may exercise all the powers of the Commissioner as delegated except for the powers to:

(i) appoint authorised officers (Section 6)
(ii) designate CII (Section 7)
(iii) withdraw designation of CII (Section 9)
(iv) take possession of computers or equipment for the purpose of carrying out further examination of analysis during serious cybersecurity incidents (Section 20)

For the power to issue written directions (Section 12), the Assistant Commissioner will be administratively empowered to issue written directions within his/her sector for operational expediency.

7. Do sectoral regulations have cybersecurity requirements? Are these requirements comparable to the powers in the Cybersecurity Act?

A few sectors such as the Banking and Finance sector have regulatory levers to tackle cyber threats and incidents. For example, MAS has Guidelines on Technology Risk Management (TRM), as well as the MAS Notice on TRM (pursuant to Section 55 of

Banking Act which empowers MAS to impose requirements on banks). The TRM Notice imposes obligations on credit card or charge card licensees to make reasonable efforts to maintain a high availability of critical systems, to establish a recovery time objective for each critical system, to notify MAS of a relevant incident, to submit a root cause and impact analysis report to MAS of the relevant incident, and to implement IT controls to protect customer information from unauthorised access or disclosure. Therefore, in these aspects, MAS's existing powers are similar to the powers over CII owners in the Cybersecurity Act.

However, most sectors have outcome-based legislation, in which penalties apply after performance or service standards fall. The Act thus provides a common set of powers to Assistant Commissioners appointed from such sector leads to empower them to enforce cybersecurity requirements within their sectors.

8. What happens if an entity breaches both the Cybersecurity Act and the Sector Lead's own Act / existing frameworks on cybersecurity? Will CSA or the Sector Lead take action?

If the directions are issued drawing powers from the Cybersecurity Act, enforcement actions for any non-compliance should be taken by the Assistant Commissioner in consultation with the Commissioner as per the penalty framework under the Cybersecurity Act.

The Cybersecurity Act does not prevent Sector Leads from setting more stringent cybersecurity requirements under their sectoral regulations to cater to the cybersecurity needs of the sector. In such cases, the sectoral regulations would take precedence over the Cybersecurity Act.

Section III: Protection of Critical Information Infrastructure

9. What is the profile of the critical information infrastructure (CII) in Singapore?

CSA has worked closely with Sector Leads to identify CII supporting the provision of essential services across 11 critical sectors.

The critical sectors are Energy, Water, Banking & Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), Government, Infocomm, Media, and Security & Emergency Services. The list of essential services in these sectors are published in the First Schedule of the Act.

Under Section 7 of the Act, critical information infrastructure (CII) refers to specific computers and computer systems that are explicitly designated by the Commissioner of Cybersecurity. It is not the case that firms and sectors will be considered as CII.

The list of CII and CII owners will be finalised, before CSA and Sector Leads implement the Cybersecurity Act in the second half of 2018. The list of CII and CII owners are secret for national security reasons.

10. **How vulnerable are our CII? Have any of our CII networks been compromised or experienced attacks?**

As a hyper-connected business hub, Singapore is vulnerable to cyber-attacks which are increasing in scale and sophistication. While we were fortunate to have escaped relatively unscathed so far, we have seen our share of cyber-attacks. One example is the breach of MINDEF's I-net system in February 2017 where the personal data of 850 national servicemen were leaked. In May 2017, Advanced Persistent Threat (APT) actors targeted two of our top universities.

Although none of our CII has been disrupted, the global WannaCry and Petya malware attacks, which also surfaced in Singapore, are reminders of our vulnerability. We can expect more attempts to breach our cyber defences.

To enhance our defences against increasingly sophisticated cyber-attacks, CSA works closely with Sector Leads to ensure that CII owners have capabilities and measures to detect, respond to and recover from cyber threats and cyber-attacks. CSA has been advocating that organisations should take cybersecurity into consideration when designing systems and networks to develop robust systems with defences against attacks, and not add them later as an afterthought.

11. **How does CSA determine the list of essential services?**

In arriving at the list of essential services in the Cybersecurity Act, CSA took reference from the list of critical sectors in the Computer Misuse and Cybersecurity Act (CMCA). CSA also surveyed the definition of "essential services" in other jurisdictions.

CSA then identified a total of 11 sectors with Critical Information Infrastructure. For each of these 11 sectors, CSA worked with the relevant Sector Lead to identify their essential services based on criteria such as impact to Singapore's economy.

We do not preclude gazetting new essential services in the future.

12. **Section 7 of the Act states that a CII is designated for a period of 5 years. Why is there a duration period for a CII?**

Over 5 years, many aspects of the CII may have changed – business, industry, clientele and market share. Hence, it would be useful to re-evaluate the status of a CII from time to time.

13. **Section 9 states that designation of a CII may be withdrawn. Can you explain with a scenario to illustrate how such a situation could arise?**

For example, if the market share served by a CII drops to below a certain threshold (e.g. a certain percentage) such that it is no longer significant, or the CII is decommissioned, the designation may be withdrawn.

14. **Why is there a need to inform the Commissioner of a change in ownership of the CII after the change has been effected?**

When the ownership of a CII changes, the new owner could have a different business case for the CII. The intent for requiring CII owners to inform the Commissioner of changes in ownership is to allow the Commissioner to assess whether the business function of the CII has changed and if the CII continues to fit the criteria of a CII. There is no intention for the Commissioner to veto any changes in ownership as these are business decisions.

Section IV: Investigation of Cybersecurity Threats and Incidents

15. **Do the new enforcement powers allow CSA to investigate and prosecute foreign hackers/organised groups attacking Singapore from overseas?**

The Cybersecurity Act deals with cybersecurity, and only extends to computers which are located wholly or partly in Singapore.

The Singapore Police Force (SPF) and the Ministry of Home Affairs (MHA) are empowered under the Computer Misuse and Cybersecurity Act (CMCA) to investigate and prosecute perpetrators of cybercrime.

Cross-border cyber-attacks and cybercrime are increasingly common. Hence, the CMCA was amended in April 2017 to allow the Police to pursue investigations into several CMCA offences that are committed from overseas, if such offences are deemed to cause, or to create a high risk of serious harm to Singapore.

With these legislative changes, Police are now able to initiate investigations against cybercriminals located overseas, by collaborating with their foreign counterparts to provide and share evidence of such cases. Where possible, Police will work towards extraditing these offenders to Singapore, and prosecuting them in Singapore courts.

Cross-border enforcement of cybercrime is challenging. The scope of extraterritorial jurisdiction in the CMCA has been very tightly scoped, to ensure that Police resources are not over-committed to pursue crimes that have limited or no impact on Singapore.

16. **Are there countries which have domestic cybersecurity legislation that provides for extraterritorial powers?**

Some countries may provide for extraterritorial powers in their cybersecurity or cybercrime legislation, to enforce cybersecurity measures or to allow for the prosecution of overseas cyber-attackers.

However, enforcement of domestic laws beyond the local jurisdiction remains a challenge. Instead, CSA would work closely with our foreign counterparts, such as through information sharing arrangements, to facilitate cybersecurity investigations.

Section V: Sharing of Cybersecurity Information

17. **How does CSA share cybersecurity information with the industry and wider public?**

The Act allows the Commissioner to request specific information from CII owners (Section 10) and during investigations of cybersecurity threats and incidents (Sections 19 and 20). The sharing of such information is an important part of protecting our systems from cybersecurity threats.

CSA also shares information on cybersecurity threats and vulnerabilities with the CII sectors so that appropriate actions can be promptly taken. This is actionable information and is often technical and operational in nature. Examples include technical indicators or signatures of the cyber threat and contextual cyber threat assessments.

Beyond CII, the Singapore Computer Emergency Response Team, or SingCERT, which is part of CSA, routinely issues timely advisories and alerts to the general public and advises on measures that the public can take to protect themselves. Information and educational materials that promote cyber hygiene for the general public are also available on the Gosafeonline website. CSA also publishes an annual Singapore Cyber Landscape report for public awareness.

The CERTs overseeing specific sectors also issue advisories to the operators in their respective sectors. For example, the Info-communications Singapore CERT, or ISG-CERT, issues alerts to operators in the telecommunications and media sector to enhance their cyber readiness, and advisories on cybersecurity vulnerabilities pertaining to this sector.

SingCERT also works with the sectoral CERTs, where necessary, to inform local companies and affected customers on cybersecurity threats and incidents. For example, when D-Link routers were found to have security vulnerabilities in September 2017, SingCERT and ISG-CERT issued a joint advisory which contained information on the affected products and the steps that affected consumers should take - for example, disable remote management of their router and use strong passwords for their Wi-Fi to minimise the risk of their device being compromised.

18. **Are there additional efforts beyond legislation to encourage the sharing of cybersecurity information?**

Facilitating information sharing will help to improve cybersecurity as timely cyber threat information will help the Government identify vulnerabilities and prevent cyber incidents more effectively.

Beyond the Act, MCI and CSA will explore implementing administrative arrangements and partnerships to facilitate and encourage information sharing. For example, MAS collaborated with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to set up the latter's regional centre in Singapore for the purpose of sharing information on threats including cybersecurity threats among financial institutions.

Section VI: Licensing of Cybersecurity Service Providers

19. **Globally, Singapore would be one of the first countries to license cybersecurity service providers. What are some views from such providers?**

There is a breadth of views from cybersecurity service providers. Some welcome the regulation, as it professionalises the industry at a time when more organisations are searching for and consuming cybersecurity services. However, there were some who expressed concerns that licensing regime could increase the operational costs of service providers and impact the development of a vibrant cybersecurity ecosystem in Singapore. In response to concerns, CSA has simplified the licensing regime following consultation, such as by doing away with the need for specific licensing of individual practitioners

20. What are CSA's justifications for introducing the licensing framework?

The licensing framework is only one part of CSA's overall strategy to develop and strengthen the cybersecurity industry in Singapore. It will be complemented by CSA's partnerships with the industry and professional association partners to establish voluntary accreditation regimes for cybersecurity professionals.

CSA's considerations for the licensing framework are to help:

(i) Provide greater assurance of security and safety to consumers of cybersecurity service providers, as such services become more common and sought after;
(ii) Raise the quality of the standards of these service providers over time; and
(iii) Address information asymmetry between service providers and consumers of cybersecurity services.

21. Why did CSA decide to license only providers of penetration testing and managed security operations centre (SOC) services?

CSA intends to adopt a light-touch approach to license penetration testing and managed security operations centre (SOC) monitoring because these services:

(i) Have access to sensitive information from their clients and could have significant impact if not delivered well or misused, and
(ii) Are also relatively mainstream in our market and hence have a significant impact on the overall security landscape.

CSA will continue to monitor international and industry trends and assess if new types of cybersecurity services are considered high-risk, and evaluate whether the providers of such services should be licensed.

22. What are the licensing conditions that licensed cybersecurity service providers have to comply with?

We intend to keep licensing requirements simple to minimise the operational costs on businesses. The requirements that licensed service providers have to comply with include:

(i) Ensure that their key executive officers performing the licensable services are fit and proper persons as defined in S26(8). For example, ensure that the individual has not been convicted of any offence involving fraud, dishonesty or moral turpitude.

(ii) Keep for at least 3 years, basic records on the cybersecurity services that it has provided. This was reduced from the earlier proposed 5 years, so as to lighten the administrative requirements on licensed cybersecurity service providers.

23. When will the licensing framework be implemented?

The licensing framework is expected to be implemented in the second half of 2019.

Section VII: Cost Implications for Businesses

24. What are the costs that CII owners and other businesses have to incur in implementing cybersecurity measures? Are there any measures to ensure that compliance costs do not trickle down to consumers?

Cybersecurity is a collective responsibility, and we must all do our part. Much of the cost of strengthening cybersecurity protection and enhancing responses to cybersecurity threats and incidents at the national level are borne directly by the Government. This includes resourcing national-level cybersecurity infrastructure and manpower, conducting regular cybersecurity exercises to validate cybersecurity incident management processes, and deploying National Cyber Incident Response Teams (NCIRT) to respond to cybersecurity incidents.

Today, many CII owners have already put in place cybersecurity measures arising from regulations in sectors such as banking and finance and infocomm. The Act aims to strengthen the cybersecurity of CII in all sectors, including those that currently do not have any cybersecurity requirements. The requirements under the Act have been carefully scoped and are considered not too onerous.

There will be cost implications for some CII owners who will have to strengthen the cybersecurity posture of their computer systems to meet the requirements of the Act. To minimise regulatory costs, we will work with sector regulators to streamline the cybersecurity audit and incident reporting processes in order to harmonise cybersecurity requirements under the Act and in their respective sectors, wherever possible.

It is also in the interest of CII owners and their vendors to spend adequately on cybersecurity measures. They should consider not only the upfront cost of such measures, but also the cost of potential breaches, including the intangible costs arising from any damage to their reputation. If organisations follow good security-by-design practices, they will spend less overall in the long-run to fix cybersecurity issues.

Section VIII: Public Awareness and Assistance relating to Cybersecurity Incidents

25. How is the Government helping to raise public awareness on the importance of cybersecurity?

CSA co-chairs the Cyber Security Awareness Alliance with the Singapore Infocomm Technology Federation (SITF). The Alliance comprises members from public, private sector and trade associations, to raise awareness and adoption of essential cyber

security practices among businesses and the community. Alliance members have been active in giving talks to schools, public and the business community to speak on the importance of cybersecurity and provide related advice.

CSA also spreads cybersecurity awareness messages at various partner events such as the Total Defence exhibition “The Power of 1”, Silver IT Fest, Tech Saturday Upsized, and crime prevention roadshows.

Aside from running annual public awareness campaigns and roadshows, CSA also collaborates with the Personal Data Protection Commission (PDPC) and the Ministry of Education (MOE) on a series of activity books to educate students on cybersecurity and other issues on internet safety issues. These activity books are also available on MOE’s online learning portal for students.

As for the elderly, the Silver Infocomm Junctions (SIJs) under IMDA teach senior citizens on how to stay safe in a digital world including sharing of information on cybersecurity.

26. How does CSA help companies and the public with regard to cybersecurity incidents?

The Singapore Computer Emergency Response Team (SingCERT) under CSA facilitates the detection, resolution and prevention of cybersecurity incidents. SingCERT achieves these objectives by:

(i) Broadcasting alerts, advisories and security patches;
(ii) Promoting cybersecurity awareness through seminars and workshops; and
(iii) Collaborating with other CERTs to respond to cybersecurity incidents.

Businesses and the public can sign up for alerts at https://www.csa.gov.sg/singcert or seek SingCERT’s advice on how to remediate cybersecurity incidents. The types of incidents that can be reported to SingCERT include:

(i) Unauthorised attempts (either failed or successful) to gain access to your system or its data;
(ii) A denial of service (DoS) attack on your IT network; and
(iii) Phishing or scam emails sent to your network.