EMBARGOED UNTIL MCI COS 2022

MEDIA FACTSHEET

Review of the Cybersecurity Act *and* Update to the Cybersecurity Code of Practice for CIIs

The Cyber Security Agency of Singapore (CSA) has embarked on two new initiatives to enhance the cyber resilience of Critical Information Infrastructure (CII[1]) sectors and better secure Singapore's cyberspace. These initiatives are (a) review of the Cybersecurity Act (CS Act) to update it for the fast-changing digital world - to improve Singapore's cybersecurity posture and support our digital economy and way of life; and (b) update of the Cybersecurity Code of Practice (CCoP) for the 11 CII sectors to better deal with new and emerging threats such as ransomware and domain-specific risks such as 5G.

2 The Government will take the lead and enhance its cybersecurity governance to address new and emerging cyber threats in the wake of strategic and technological shifts.

Review of the Cybersecurity Act

3 The Cybersecurity Act, which came into force on 31 August 2018, establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Since its introduction, reliance on digital infrastructure and services has increased significantly. As Singapore digitalises, more organisations are now at risk of falling victim to cyber-attacks if the necessary cybersecurity safeguards are not put in place. CSA is therefore reviewing the CS Act to ensure that the digital infrastructure and services that we use are secure.

4 The CS Act has thus far focused on CIIs, which support the delivery of essential services in the physical world such as water and power. Moving forward, CSA will explore expanding the CS Act to improve awareness of threats

[1] CIIs are computer systems that support the delivery of essential services. Today, CIIs have been identified from 11 critical sectors — Aviation, Banking & Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security & Emergency Services and Water.

over Singapore's cyberspace, protect virtual assets (e.g. systems hosted on the cloud) as CII if they support essential services. Beyond the CIIs, the CS Act review will also cover foundational digital infrastructure and key digital services, e.g. apps, that are important to enable our Digital Economy and sustain our Digital Way of Life.

5 Given that the review may affect various parties in the cybersecurity landscape, CSA will be consulting relevant stakeholders on the proposed amendments and will also conduct a public consultation in early 2023 to solicit views from the wider community. More details will be shared in due course.

Update to the Cybersecurity Code of Practice

6 The Cybersecurity Act provides a framework for the designation of CII, and CII Owners across the 11 critical sectors are required to comply with the mandatory cyber hygiene practices within the CCoP [2] to ensure a strong cybersecurity foundation for the CII sectors. In December 2019, a set of mandatory Operational Technology (OT)-specific cybersecurity practices was introduced as an addendum to the CCoP with the aim of elevating the state of cybersecurity for OT CII.

7 However, as cyber threats continue to evolve and grow in sophistication, foundational cyber hygiene practices may no longer be sufficient for CII Owners to defend against such threats. In particular, ransomware has evolved into a massive and systemic threat which can pose concerns to national security and disrupt critical services. Additionally, every CII sector faces cybersecurity risks that are specific to their digital terrains e.g., migration to the Cloud or use of 5G technologies. Cyber hygiene practices that are generic across critical sectors would not be able to address such specific risks.

8 CSA intends to enhance the existing CCoP to achieve the following three objectives:

a. To help CIIs improve their odds of defending against cyber threat actors using sophisticated threats;
b. To allow CIIs to be more agile to respond to emerging risks in specific domains; and

[2] CCoP is a list of Codes of Practice issued by the Commissioner of Cybersecurity for the regulation of CII Owners in accordance to the Cybersecurity Act.

c. To enhance coordinated defences between Government and private sectors to identify, discover and respond to cyber threats and/or attacks in a timely manner.

9 Key CII stakeholders comprising CII Sector Leads and CII Owners were briefed and consulted on the enhanced CCoP. Examples of the enhancements include:

a. Adopting a threat-based approach to identify threat actors' common tactics and techniques used in a cyber-attack lifecycle. This will allow CSA to identify actions, develop new practices and/or enhance existing practices to counter and impede the threat actors' activities in a cyber-attack; and

b. Allowing the flexibility to add domain-specific practices, e.g. use of 5G technologies, on an ad-hoc basis to the relevant CII sectors and/or specific CII Owners to implement. This will help to increase sectors' agility in addressing emerging risks.

Their feedback will be factored in before the enhanced CCoP is issued to CII Owners in Q2 2022.