ANNEX A

MEDIA FACTSHEET

CYBER ESSENTIALS & CYBER TRUST MARKS

Cyber-attacks on the global supply chain could bring about devastating downstream economic and social ramifications in this interconnected and digital world. Cyber-attackers do not just steal enterprises' business and customer data, but could also threaten enterprises by "locking up" IT infrastructure and data for ransom. In this digital economy, businesses and consumers will benefit with the increased trust and confidence from transacting with organisations that have prioritised cybersecurity.

2 The **Cyber Essentials** mark recognises enterprises that have put in place cyber hygiene measures, while the **Cyber Trust** mark is a mark of distinction to recognise enterprises with comprehensive cybersecurity measures and practices. The marks do not certify the cybersecurity of specific products or services, but rather, they certify the cybersecurity measures adopted at the organisation level. The two cybersecurity certification marks were developed in consultation with industry partners such as certification practitioners, technology providers and trade associations and take into consideration the diverse organisational profiles and operational needs of enterprises in Singapore.

Cyber Trust

3 The Cyber Trust mark is targeted at larger or more digitalised enterprises - such as Multinational Corporations (MNCs) – as these enterprises are likely to have higher risk levels which require them to invest in expertise and resources to manage and protect their IT infrastructure and systems. It adopts a risk-based approach to guide enterprises to understand their risk profiles and identify relevant cybersecurity preparedness areas required to mitigate these risks. The Cyber Trust mark comprises five Cybersecurity Preparedness tiers that correspond to the enterprise's risk profile. Each tier consists of 10 to 22 domains in areas such as cyber governance and oversight, cyber education, information asset protection, secure access and environment, and cybersecurity resilience in order to assess the cybersecurity posture of the enterprise.

4 For example, a financial services institution has to ensure its internal and external systems have a robust level of cybersecurity to protect the treasure trove of its customers' personal and financial data. The organisation's investments and efforts in cybersecurity will be recognised and certified under the Cyber Trust mark. The certification gives the company a competitive advantage and provides assurance and peace of mind for its customers.

Cyber Essentials

5 The Cyber Essentials mark recognises enterprises that observe good cyber hygiene. It is targeted at organisations such as Small and Medium Enterprises (SMEs). Such enterprises tend to have limited IT and/or cybersecurity expertise and resources, and the Cyber Essentials

mark aims to enable them to prioritise the cybersecurity measures needed to safeguard their systems and operations from common cyber-attacks. These baseline measures include preventative measures to protect and control access to systems/data, back up data and update software, as well as responding to a cyber incident.

6 An example of a company that would benefit from the Cyber Essentials mark is an SME F&B firm with its own customer loyalty programme. The firm would possess personal data of its customers such as name, date of birth, etc., and would have implemented baseline cybersecurity measures such as controlling access to and backing up customer data, as well as investing in software to protect its internal IT systems.

7 The Cyber Security Agency of Singapore (CSA) will work with its industry partners such as SGTech to encourage adoption of both cybersecurity marks. The certification process will be undertaken by certification bodies that have been appointed by CSA. For a start, CSA has appointed the following eight certification bodies:

- BSI Group Singapore Pte Ltd
- Bureau Veritas Quality Assurance Pte Ltd
- EPI Certification Pte Ltd
- exida Asia Pacific Pte Ltd
- Guardian Independent Certification Pte Ltd
- ISOCert Pte Ltd
- SOCOTEC Certification Singapore Pte Ltd
- TÜV SÜD PSB Pte Ltd

Applicants may refer to CSA’s website for more details on the appointed Certification Bodies’ respective offerings, application process and fees: www.csa.gov.sg/cyber-certification.

8 Both cybersecurity marks are initiatives under CSA’s **SG Cyber Safe Programme** targeted at enterprises. Announced during the Ministry of Communications and Information (MCI)’s Committee of Supply (COS) in March 2021, the SG Cyber Safe Programme is one of the major initiatives under CSA’s Safer Cyberspace Masterplan. The Masterplan aims to increase the general level of cybersecurity awareness and drive adoption of good cyber practices by individuals, businesses and the larger community. The SG Cyber Safe Programme targets specifically businesses and enterprises to raise their cybersecurity awareness, equip them with relevant tools and resources to take action in raising their enterprise cybersecurity posture, and encourage cybersecurity adoption.

###

About the Cyber Security Agency of Singapore

Established in 2015, the Cyber Security Agency of Singapore (CSA) seeks to keep Singapore’s cyberspace safe and secure to underpin our Nation Security, power a Digital Economy and protect our Digital Way of Life. It maintains an oversight of national cybersecurity functions and works with sector leads to protect Singapore's Critical Information Infrastructure. CSA also engages with various stakeholders to heighten cyber security awareness, build a vibrant cybersecurity ecosystem supported by a robust workforce, pursue international partnerships and drive regional cybersecurity capacity building programmes.

CSA is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information. For more news and information, please visit www.csa.gov.sg.

For media enquiries, please contact:

Tan Boon Leng
Senior Assistant Director, Comms and Engagement Office
Email: Tan_Boon_Leng@csa.gov.sg

Elaine Lim
Senior Manager, Comms and Engagement Office
Email: Elaine_Lim@csa.gov.sg