MEDIA FACTSHEET

CYBERSECURITY LABELLING SCHEME

1 The Cyber Security Agency of Singapore (CSA) has launched the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, as part of efforts to improve Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore's cyberspace.

2 The CLS is the first of its kind in the Asia-Pacific region. Under the scheme, smart devices will be rated according to their levels of cybersecurity provisions. This will enable consumers to identify products with better cybersecurity provisions and make informed decisions.

3 The CLS also aims to help manufacturers stand out from their competitors and be incentivised to develop more secure products. Currently, consumer smart devices are often designed to optimise functionality and cost. They also have a short time-to-market cycle, where there is less scope for cybersecurity to be incorporated into product design from the beginning.

4 For a start, CSA will introduce the CLS to Wi-Fi routers and smart home hubs. These products are prioritised because of their wider usage, as well as the impact that a compromise of the products could have on users. The Government is also taking the lead, with CSA and other government agencies working together to adopt the CLS for their smart devices.

Details of the Scheme

5 The CLS is a voluntary scheme. It comprises four levels of rating, represented by one, two, three, or four asterisks. Each additional asterisk represents an additional tier of testing and assessment that the product has undergone. The general requirements for each level are as follows:

Level	Requirement
Level 1	The product meets basic security requirements such as ensuring unique default passwords and providing software updates.
Level 2	The product has been developed using the principles of Security-by-Design such as conducting threat risk assessment, critical design review and acceptance tests, and fulfilled Level 1 requirements.
Level 3	The product has undergone assessment of software binaries by approved third-party test labs, and fulfilled Level 2 requirements.

Level 4	The product has undergone structured penetration tests by approved third-party test labs and fulfilled Level 3 requirements.

6 Manufacturers applying for the first two levels will need to submit a declaration of compliance with supporting evidence, while those applying for Levels 3 and 4 will also be required to submit the assessment report by an approved lab. The cybersecurity label will be valid for the length of time for which the device will be supported with security updates, up to a maximum of 3 years.

7 The CLS takes reference from the European Standard EN 303 645 'Cyber Security for Consumer Internet of Things: Baseline Requirements'.

8 To encourage adoption of the scheme, CSA will waive the application fees for the CLS for a year.

9 The CLS is an initiative under the Safer Cyberspace Masterplan 2020, which is a blueprint for the creation of a safer and more secure cyberspace in Singapore.

10 For more details on the CLS, please visit www.go.gov.sg/csa-cls.

-END-

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.

Appendix

Example of a Level 1 cybersecurity label