Annex C

Fact Sheet

IoT Cyber Security Guide Public Consultation

IoT technology will play an important role in Singapore's journey to become a digital economy, with inter-connected IoT devices, systems and networks generating valuable data that can be used to help transform businesses and enhance public's lifestyle and well-being.

With increased deployment of IoT devices and systems, and to foster greater confidence in users of IoT services, it is important that IoT devices and systems are properly secured to prevent service disruptions and data breaches.

IMDA has thus launched a public consult on the 25 January to seek views and comments on its proposed IoT cybersecurity guide. This guide will list baseline recommendations for procuring and operating IoT systems, covering the life cycle of the systems, to help organisations make better equipment purchasing and deployment decisions, by taking security designs into consideration.

In addition, the guide offers two checklists to help deploying organisations systematically assess the security state of their IoT systems to determine if sufficient protection from unintentional and malicious threats have been put in place. In particular, the threat modelling checklist assists organisations to identify and understand the potential vulnerabilities/threats in the systems and the vendor disclosure checklist helps organisations to ensure the IoT systems procured are adequately secured.

Smart home-related use cases within the guide will also help IoT vendors develop better products and solutions to benefit Singapore homeowners.