

Secure by Design – UK-Singapore IoT Statement

At the Commonwealth Heads of Government Meeting in April 2018, Singapore along with 52 nations, through the Commonwealth Cyber Declaration agreed to commit to work towards the development and convergence of approaches for internet-connected devices and associated services, in order to promote user security by default.

As part of the Singapore-UK Strategic Partnership, it was agreed that the two countries would work together on areas of common interest including greater cooperation, alignment and coordination to support a global consensus for 'secure by default'. In 2018, Prime Minister Lee Hsien Loong and Prime Minister Theresa May agreed to launch the SG-UK Partnership for the Future and formally launched in January 2019 by the UK's Foreign Secretary Jeremy Hunt and Singapore's Minister for Foreign Affairs Dr Vivian Balakrishnan.

Singapore and the UK endeavour to take a leading role in driving improvements in the security of smart consumer products. We want to ensure that internet-connected devices have security built in by design and the public and industry are protected against related security threats, such as cyber attacks, theft of personal data and risks to physical safety.

At the same time, we must ensure that IoT industry can continue to grow and innovate and the public can fully benefit from these products and services.

UK and Singapore have committed to share initiatives and approaches, and to exchange valuable information and experience in order to make tangible progress.

Both nations will adopt a multilateral approach by working with our partners, both internationally and regionally, including industry and consumer groups, to promote the implementation of good practice as set out in the relevant industry global standards. Implementing clear good practice principles from Industry across all their consumer IoT devices will result in citizens and the wider economy being made safer and more secure whilst using their products. UK and Singapore recommend that manufacturers implement industry best practices such as:

1. Discontinuing the most blatant security shortcomings, such as the use of universal default passwords.
2. Normalising vulnerability disclosure processes across the IoT industry, so that researchers can report security vulnerabilities and manufacturers can respond accordingly.
3. Encouraging the development and deployment of software security updates so that consumers and the wider technical ecosystem are protected throughout the entire life-time of IoT products. Manufacturers should define a support period for the fixing of vulnerabilities.

We support the development of IoT assurance schemes and other efforts designed to give consumers confidence in the security of their products. The UK and Singapore have a shared interest in enhancing our bilateral cooperation in this area, as we develop our national approaches.

We are committed to strengthening our dynamic partnership for the 21st Century. We cooperate closely around the world. The UK and Singapore will work together with our partners and stakeholders to protect and promote the safety of our citizens and the security of our economies.

Singapore and the United Kingdom will continue to strengthen cooperation and explore options for further collaboration, including through the sharing of best practices.