Joint statement of intent from the for Agile Nations Working Group on Cyber Security for Consumer Connected Products

News story

UK, Canada and Singapore agree to work together to promote and support cyber security measures for internet connected products.

The continued growth in network connectable (also known as Internet of Things, or ‘IoT’) products offers great benefits to citizens, and a revolution in connectivity. However, many of these products currently lack even basic cyber security provisions. The result is that consumers’ security, privacy and safety are at risk, with the wider economy vulnerable to large-scale cyber-attacks that can be launched through insecure IoT.

The governments of Canada, Singapore and the United Kingdom are united in our belief that connected products offer tremendous economic and social benefits, and that appropriate cyber security requirements must be built into these products from the design stage, rather than placing this burden on consumers. Our approach supports growth and innovation, and allows citizens to benefit from the remarkable opportunities offered by this connected revolution.

To protect consumers across the globe requires coordinated efforts from like-minded governments, academia, and civil society. Our three governments are working together to promote and support the development of international standards and industry guidance, to foster innovation, and to encourage approaches that incorporate internationally recognised security requirements and avoid fragmentation. Through this global alignment we can reduce duplication of testing and similar assessments and the challenge for industry of needing to apply to multiple schemes underpinned by identical or very similar requirements.

We endorse the emerging baseline security requirements for these products,

and encourage international recognition and alignment with them. We are united in our view that international standards can facilitate strong security practices and we encourage the adoption of international standards to mitigate these cyber risks. We are committing to continue working closely together, and we will continue to promote global alignment on best practices and encourage the recognition of aligned schemes to reduce unnecessary barriers to trade and industry.

Published 10 November 2022