WORLD TRADE ORGANIZATION

G/TBT/N/GBR/44

29 November 2021

(21-8975)

Page: 1/3

Committee on Technical Barriers to Trade

Original: English

NOTIFICATION

The following notification is being circulated in accordance with Article 10.6

1. **Notifying Member:** UNITED KINGDOM

If applicable, name of local government involved (Article 3.2 and 7.2):

2. **Agency responsible:** Department for Digital, Culture, Media and Sport (DCMS)

Name and address (including telephone and fax numbers, email and website addresses, if available) of agency or authority designated to handle comments regarding the notification shall be indicated if different from above:

UK TBT Enquiry Point
Trade Policy Group
Department for International Trade
Old Admiralty Building
London
SW1A 2DY
TBTEnquiriesUK@trade.gov.uk

3. **Notified under Article 2.9.2 [X], 2.10.1 [ ], 5.6.2 [ ], 5.7.1 [ ], other:**

4. **Products covered (HS or CCCN where applicable, otherwise national tariff heading. ICS numbers may be provided in addition, where applicable):** This notification is in reference to the cyber security of consumer connectable products defined as a 'internet-connectable' product or a 'network-connectable' product made available to consumers in the UK. This relates to the HS Code List of Chapter 84 and 85. In scope products include but are not limited to: - smartphones - connected cameras, TVs and speakers - connected children's toys and baby monitors - connected safety-relevant products such as smoke detectors and door locks - Internet of Things base stations and hubs to which multiple devices connect - wearable connected fitness trackers - outdoor leisure products, such as handheld connected GPS devices that are not wearables - connected home automation and alarm systems - connected appliances, such as washing machines and fridges - smart home assistants Laptops, PCs, medical devices, tablets without a cellular connection, smart charge points, automotive vehicles and smart meters/other smart metering products are out of scope. This list is non-exhaustive and will be developed further via regulations.

5. **Title, number of pages and language(s) of the notified document:** Product Security and Telecommunications Infrastructure Bill (72 page(s), in English)

6. **Description of content:** The UK's Product Security and Telecommunications Infrastructure Bill creates a new regulatory scheme to ensure that consumer connectable products are more secure against cyber attacks. Part 1 of this bill mandates that minimum cyber security requirements must be adhered to in relation to consumer connectable products sold in the UK. This bill provides a robust regulatory framework that can adapt and remain effective in the face of rapid technological advancement, the evolving techniques employed by malicious actors, and the broader international regulatory landscape.

The UK notified a public consultation for this measure on 24 August 2020 as "Proposal for Cyber Security of Consumer IoT Devices" (G/TBT/N/GBR/36) with a corrigendum (G/TBT/N/GBR/36/Corr1).

7. **Objective and rationale, including the nature of urgent problems where applicable:** Consumer connectable products (also known as consumer Internet of Things (IoT)) are becoming commonplace in millions of homes around the world and uptake of these products increased further as a result of the COVID-19 pandemic. Many of these products on the market today still have basic flaws, such as universal default passwords, which leave them vulnerable to cyberattacks such as DDoS (Distributed Denial of Service) attacks. Cyber criminals are increasingly targeting these products with Kaspersky reporting that there were 1.5 billion attempted compromises of IoT (Internet of Things) devices in the first half of 2021. This is double the number of reported attacks in the same period in 2020 and highlights that urgent intervention is needed to protect the security and privacy of UK consumers and the UK's digital infrastructure. Similarly, the proportion of manufacturers selling connectable products who maintain a coordinated vulnerability disclosure programme has increased from 9.7% (2018) to 18.9% (2020) to 21.6 % in 2021 but this is still unacceptably low and represents an inability to properly respond to vulnerabilities that can have real world consequences. The UK government's Product Security and Telecommunications Infrastructure Bill represents widely recognised good practice, and regulation was strongly supported in a 2019 consultation on regulatory options. The UK government has worked in partnership with other countries and international organisations. Since 2018, DCMS have worked in partnership with ETSI (European Telecommunications Standards Institute), to develop Technical Specification 103 645 in February 2019, and European Standard (EN) 303 645 v2.1.1 in June 2020. These outputs are the product of intense feedback from representatives from up to 65 countries. In addition, the UK government has worked in partnership with other governments to raise the profile of this issue and continues to seek to deliver alignment and avoid fragmentation. In 2019, representatives from the UK, USA, New Zealand, Canada and Australia published a 'five country ministerial statement' outlining their shared commitment to improving the security of connectable products in their respective domestic markets. Through the IoT Security Platform the UK government works with foreign governments and industry members including Arcep (France), ISED (Canada), MCTPEN (Senegal), AGESIC (Uruguay), METI (Japan), New Zealand, NIST (USA). More recently, the UK has worked closely with the governments of Singapore, Australia and India, all of whom have now initiated their own domestic schemes or have published Codes of Practice for Securing Consumer IoT. ; Other

8. **Relevant documents:**

The latest version of the Product Security and Telecommunications Infrastructure Bill can be found here: https://bills.parliament.uk/bills/3069 but a PDF document has also been provided.

1. Impact Assessment from the Department for Digital, Culture, Media and Sport can be found here: https://bills.parliament.uk/publications/43916/documents/1025
2. Proposals for regulating consumer smart product cyber security - call for views 2020: https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views
3. The government response to that call for views can be found here: https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response

9. **Proposed date of adoption:** Anticipated to receive royal assent in 2022

Proposed date of entry into force: Anticipated in 2023

10. **Final date for comments:** Comments can be submitted via the UK's Enquiry Point and will be considered up until 60 days from 27.11.2021.

11. Texts available from: National enquiry point [X] or address, telephone and fax numbers and email and website addresses, if available, of other body:

UK TBT Enquiry Point
Trade Policy Group
Department for International Trade
Old Admiralty Building
London
SW1A 2DY
TBTEnquiriesUK@trade.gov.uk

https://members.wto.org/crnattachments/2021/TBT/GBR/21_7390_00_e.pdf