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 PointTrade Policy GroupDepartment for International Trade3 Whitehall PlaceLondonSW1A 2AWTBTEnquiriesUK@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 Internet of Things (IoT) products defined as any network-connectable product and their associated services that are supplied or made available within the UK. This relates to the HS Code List of Chapter 84 and 85. Products may include, but are not limited to: connected children's toys and baby monitors, connected safety-relevant products such as smoke detectors and door locks, smart cameras, TVs and speakers, wearable health trackers, connected home automation and alarm systems, connected appliances (e.g. washing machines, fridges), smart home assistants, smartphones, tablets and laptops. Products that are out of scope as they are or soon will be covered by existing legislation, this includes smart metering devices that require Commercial Product Assurance (CPA), automotive including electric vehicles, and smart charge points and medical devices.; NUCLEAR REACTORS, BOILERS, MACHINERY AND MECHANICAL APPLIANCES; PARTS THEREOF (HS 84); ELECTRICAL MACHINERY AND EQUIPMENT AND PARTS THEREOF; SOUND RECORDERS AND REPRODUCERS, TELEVISION IMAGE AND SOUND RECORDERS AND REPRODUCERS, AND PARTS AND ACCESSORIES OF SUCH ARTICLES (HS 85) |
| **5.** | **Title, number of pages and language(s) of the notified document:** N/A |
| **6.** | **Description of content:** Notice is hereby given to inform WTO Members that the UK are currently carrying out an early-stage call for views on a proposed policy. An addendum to this notification will be issued alongside a draft text, expected in early 2021.DCMS published a [Call for Views](https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views) (alongside two research reports and an online feedback form) on 16 July 2020 which represents the UK's proposals for regulating the cyber security of consumer smart products.  This includes the  scope of regulation and the products included, the proposed definitions, the technical security requirements, how the requirements translate into obligations on producers and distributors of these products and the proposed enforcement approach.DCMS wish to notify WTO Members of the Call for Views document and invite feedback before 6 September 2020, either:-          As part of the Call for Views process via our online [feedback form](https://dcms.eu.qualtrics.com/jfe/form/SV_5hYgWfhEZf66l8h)-          In response to the WTO notification process via TBTEnquiriesUK@trade.gov.uk (Supportive comments or NIL returns are also welcome).Background: DCMS are proposing new legislation that will  mandate important cyber security requirements to protect citizens and the wider economy from the range of harms that could arise from vulnerable internet-connected products. The legislation would be UK wide.  The security requirements are consistent with the principles first published in the 2018 [Code of Practice for Consumer IoT Security](https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security) and is based on aspects of key provisions within the globally-applicable standard European Telecommunications Standards Institute (ETSI) [European Standard (EN) 303 645 v2.1.1,](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf) which has undergone two years of feedback and reviews from industry, academics and national standards organisations.  |
| **7.** | **Objective and rationale, including the nature of urgent problems where applicable:** Internet of Things (IoT) devices are becoming commonplace in millions of homes around the world and while forecasts vary, [research suggests](https://securityboulevard.com/2020/01/new-iot-security-regulations-what-you-need-to-know-2/) that there could be as many as 75 billion connected smart devices in homes around the world by the end of 2025. Many of the  devices on the market still have basic flaws, such as universal default passwords, which leave the devices vulnerable to DDoS (Distributed Denial of Service) attacks. Similarly, a 2019 report by the [IoTSF](https://www.iotsecurityfoundation.org/wp-content/uploads/2020/03/IoTSF-2020-Progress-Report-Consumer-IoT-and-Vulnerability-Disclosure.pdf) showed that 87% of manufacturers surveyed did not maintain a coordinated vulnerability disclosure policy, representing an inability to properly respond to vulnerabilities that can have real world consequences. Forecasts of the number of IoT devices being attacked are set to increase, with [Kaspersky](https://www.infosecurity-magazine.com/news/over-100-million-iot-attacks/) identifying 105 million attacks on IoT endpoints in 2019, increasing significantly from the 12 million detected in the first half of 2018, highlighting that urgent intervention is needed to protect the security and privacy of UK consumers. What the UK government is proposing represents widely recognised good practice, and regulation was strongly supported in a 2019 consultation on regulatory options. An updated [landscape map](https://iotsecuritymapping.uk/) was designed to ease international implementation, and also to illustrate the level of consensus on these core principles from international standards bodies and other governments. 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](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf)  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 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 IoT products in their respective domestic markets. Through the IoT Security Platform the UK government works foreign governments and industry members including Arcep (France), ISED (Canada), MCTPEN (Senegal), AGESIC (Uruguay), METI (Japan), New Zealand, NIST (USA).; Prevention of deceptive practices and consumer protection |
| **8.** | **Relevant documents:** On 16 July 2020, DCMS published a [Call for Views on proposals for regulating consumer smart product cyber security, a key document that](https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views) DCMS would invite feedback on.DCMS published a consultation on our regulatory proposals last year which advocated that all devices adhere to a baseline that is centred around aspects of the top three security requirements set out in the:* [Code of Practice for Consumer IoT Security](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf) (published by DCMS in March 2018)
* [ETSI European Standard (EN) 303 645 v2.1.1](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf) (published in June 2020 following a voting process with representatives from over 20 National Standards Organisations.

Research by [RSM UK Consulting LLP](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf) considered the potential impact of our regulatory proposal on both UK and international trade and concluded that the impact on UK trade would be minimal and made reference to international trade also. Further information on all of the above can be found on the [Secure by Design GOV.uk website](https://www.gov.uk/government/collections/secure-by-design). |
| **9.** | **Proposed date of adoption:** To be announced - anticipated late 2021/2022**Proposed date of entry into force:** To be announced - anticipated 2022 |
| **10.** | **Final date for comments:** 17 September 2020; DCMS are notifying at an early stage, therefore request comments on our proposed legislation as outlined in the Call for Views are provided via the online feedback form by 6 September 2020. Comments can be submitted and will be considered up until 17 September 2020 via the UK's Enquiry Point. DCMS will submit a further notification including our draft legislative text early next year, anticipated to be around March 2021. |
| **11.** | **Texts available from: National enquiry point [** **]** **or address, telephone and fax numbers and email and website addresses, if available, of other body:** N/A |