WORLD TRADE ORGANIZATION

G/TBT/N/AUS/176

10 October 2024

(24-7117)

Page: 1/2

Committee on Technical Barriers to Trade

Original: English

NOTIFICATION

The following notification is being circulated in accordance with Article 10.6

1.	**Notifying Member:** AUSTRALIA **If applicable, name of local government involved (Article 3.2 and 7.2):**
2.	**Agency responsible:** Department of Home Affairs **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:** Australian TBT Enquiry Point Department of Foreign Affairs and Trade Ph +61 2 6261 1111 tbt.enquiry@dfat.gov.au www.dfat.gov.au
3.	**Notified under Article 2.9.2 [X], 2.10.1 [ ], 5.6.2 [ ], 5.7.1 [ ], 3.2 [ ], 7.2 [ ], other:**
4.	**Products covered (HS or CCCN where applicable, otherwise national tariff heading. ICS numbers may be provided in addition, where applicable):** Smart devices (also known as internet-of-things devices) defined as *relevant connectable products* in the proposed Cyber Security Bill. Some examples include, but are not limited to, the following products and their HS codes (permitted they are an internet or network connectable version of that product): • Smart TV – 852872 • Wireless headphones – 851830 • Smart LED light bulbs – 853952 • Baby monitors – 852560 • Connected doorbells – 853180 • Smart vacuum cleaner - 850811
5.	**Title, number of pages and language(s) of the notified document:** Part 2, Cyber Security Bill 2024; (100 page(s), in English)
6.	**Description of content:** The proposed Australian Cyber Security Bill establishes the power for the relevant Minister to make mandatory security standards for smart devices, also known as Internet of Things (IoT) devices, under Ministerial rules. To ensure international alignment, Australia will define these devices as *relevant connectable products*, consistent with the UK definition per section 5 of the *Product Safety and Telecommunications Act 2022*. Under the Cyber Security Bill, responsible entities will be required to manufacture and/or supply smart devices in Australia in compliance with the

	relevant security standard for the specified device. Responsible entities will be required to provide a statement of compliance if requested by the Secretary of the Department of Home Affairs. Standards made under Ministerial rules could apply to all devices that meet the definition of *relevant connectable product*, or be limited to a subset, type, or class of devices, which will be defined in the relevant security standard under rules. All security standards introduced as rules under the proposed Cyber Security Bill will be subject to a 28 day consultation period prior to being introduced under this Bill.
7.	**Objective and rationale, including the nature of urgent problems where applicable:** Consumer smart devices are quickly growing in popularity and availability, with approximately 21 billion smart devices worldwide today. It is predicted there will be as many as 80 billion smart devices globally by 2025. It is estimated that over a third of Australians have added a smart device to their home in the last two years. Research has consistently shown that the rapid growth in the smart device market has outpaced the adoption of good cyber security practices. Unless security is prioritised, the growth in active apps and devices will exponentially increase risk of cyber incidents. A study by the University of New South Wales in 2020 assessed the security of a sample of consumer smart device products available to consumers locally and found that every device selected displayed basic vulnerabilities such as default passwords. These vulnerabilities are being exploited in the real world, with impacts on cyber security, privacy and online safety. Smart devices can also be used as the initial entry point to compromise the larger networks they are connected to. The increasing value of personal data, financial tokens and credentials collected through apps and stored in devices, including smart devices, will increase the incentives to target these devices. Increased online activity requires cyber secure technology and software so that consumers in Australia can transact and connect with confidence in the networks and devices that we now rely on. The proposed Cyber Security Bill will establish new powers for security standards to be made for smart devices in Australia under Ministerial rules. A rules-based model for implementing mandatory standards provides flexibility to introduce and update standards as required and supported by industry best practice. This approach will help ensure smart devices supplied in Australia are secure by design and have a level of cyber security consistent with the international market.
8.	**Relevant documents:** • Cyber Legislative Reforms Consultation Paper • 2023-2030 Australian Cyber Security Strategy and Horizon 1 Action Plan • Cyber Security Bill 2024 – Parliament of Australia (aph.gov.au)
9.	**Proposed date of adoption:** Anticipated late 2024 **Proposed date of entry into force:** 12 months from passage
10.	**Final date for comments:** 14 November 2024
11.	**Texts available from: National enquiry point [ ] or address, telephone and fax numbers and email and website addresses, if available, of other body:** Australian TBT Enquiry Point Department of Foreign Affairs and Trade Ph +61 2 6261 1111 tbt.enquiry@dfat.gov.au https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7250 https://members.wto.org/crnattachments/2024/TBT/AUS/24_06727_00_e.pdf