



25 August 2021

Cyber, Digital and Technology Policy Division
Department of Home Affairs
By email: techpolicy@homeaffairs.gov.au

Dear Sir/Madam

Re: Strengthening Australia's cyber security regulations and incentives

Standards Australia (SA) is pleased to provide a submission to the Australian Government's Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper (Discussion Paper).

Introduction

The rapid adoption of smart devices, otherwise known as Internet of Things (IoT) devices, potentially exposes consumers to pervasive and sophisticated cyber-attacks. Importantly, these devices are found in almost every home (i.e., smart TVs, watches, baby monitors) and are not the equipment the public traditionally associate with security vulnerabilities. This means that consumers have little awareness of the level of risk or protection provided by these devices, and whether the equipment is safe.

SA is pleased that the Discussion Paper notes the importance of product labelling underpinned by standards to strengthen smart device security.

As Australia's national standards development body, we recommend the Australian Government work with SA and industry - the Internet of Things Alliance Australia (IoTAA), to develop an IoT cyber security trust mark certification and labelling scheme for smart devices (IoT security trust mark scheme) as a priority initiative. IoTAA originally proposed a scheme in 2017, which was endorsed by the Prime Minister's Security Taskforce. IoTAA recently approached SA to partner on the initiative.

A cyber security trust mark certification and labelling scheme for smart devices

The establishment of an IoT security trust mark scheme requires the development or adoption of appropriate smart device cyber security standards.

Smart device standards

SA is responsible for overseeing Australian Standards® development, and the adoption of International Standards through the International Standards Organisation (ISO) and International Electrotechnical Commission (IEC). We work with industry, government, and

the community to develop and adopt standards through an open process of consultation and consensus. We invite interested parties to participate in these processes.

Our intent is to widen and deepen our engagement in cyber security, an important issue for the community, and to contribute to Australia being a leading digital economy by 2030.

We view international standards, through ISO and IEC, as a sensible pathway to protecting Australian government, businesses and consumers from cyber security, privacy, and online safety threats.

Standards can function as market enablers, and a means to achieve broader business and public policy goals on raising cyber security awareness. Standards can enable the growth of businesses, as globally embedded norms that service providers can build to, as they expand into new markets where adherence to International Standards might be beneficial.

The opportunity, and challenge, for Australian stakeholders is to effectively use the standards development process to promote, develop, and realise the opportunities of smart devices. Internationally aligned standards can help to decrease barriers to trade, ensure quality and build greater public and consumer trust in digital products and services.

Accordingly, SA recommends the Australian Government continue to support Australia's participation in cyber security standards setting internationally through SA's trusted and established processes. Standards form one element of an effective IoT security trust mark scheme.

Smart device labelling

The Australian Government has a critical role in raising awareness and promoting devices certified safe for cyber security. This is not only for its own internal use but for the widespread benefit of Australian businesses and consumers. To achieve this, the second element of an effective IoT security trust mark scheme is consumer information for smart devices provided by a certified labelling scheme.

A certified labelling scheme relies on standards to guide manufacturers on how to rate and label their products to provide assurance on the level of cyber security. A good example is the Water Efficiency Labelling Standards (WELS) scheme.



The WELS scheme has helped consumers with purchasing decisions based on water efficiency of shower heads, toilet systems, tapware, and other water-using appliances. The scheme references **Australian Standards®** which guide manufacturers towards compliance achieving the water-saving outcome. Since the introduction of the label in 2005, water efficient products have helped reduce domestic water use by 150,000 mega litres each year – enough water to fill 60,000 Olympic sized swimming pools.

Standards Australia Limited
Exchange Centre, Level 10, 20 Bridge Street, Sydney NSW 2000
GPO Box 476, Sydney NSW 2001
Telephone +61 2 9237 6000, Facsimile +61 2 9237 6010
www.standards.org.au

Under the IoT security trust mark scheme, smart devices would require independent certification before they could register. The certification would be provided by accredited independent certifying body, once it demonstrates that it conforms with Australian Standards® or adopted international standards through the SA authorisation process. Once certified, it is authorised to utilise a smart device cyber security label.

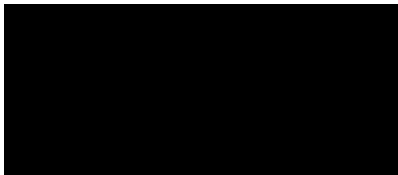
This label would provide consumers with confidence of the independently verified cyber security claims of the devices and solutions they are purchasing, while maintaining adaptability for manufacturers to implement security in accordance with need.

Recommendation

The Australian Government work with SA and industry - the Internet of Things Alliance Australia (IoTAA), to develop the IoT security trust mark scheme as a priority initiative.

We look forward to the opportunity to discuss the submission in further detail. Please contact Connie Ho, Strategic Initiatives Manager, at [REDACTED].

Yours faithfully



Adam Stingemore
General Manager, Engagement & Communications