CHOICE

1 March 2024

Department of Home Affairs
6 Chan St, Belconnen ACT 2617
cisgcomms@homeaffairs.gov.au

2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper

CHOICE welcomes the opportunity to contribute a consumer perspective on proposed secure-by-design standards for smart or Internet of Things (**IoT**) devices. As the IoT market grows, consumers expect basic security standards to protect their safety. IoT devices have significant access to user data – whether it's provided directly by the user, networked with other data-processing software or hardware, or collected through voice and/or camera technology – making them attractive targets for criminals and exploitative businesses.

CHOICE supports the government's intention to move beyond voluntary guidelines and into mandatory and enforceable standards. Mandatory standards in the development and distribution of IoT will greatly improve consumer safety. Consumers have experienced the benefits of mandatory standards in other product categories such as children's products and button batteries.

CHOICE welcomes the contribution of the Internet of Things Alliance Australia (**IoTAA**) to this consultation and supports their vision of balancing innovation in the IoT market with building trust with consumers. CHOICE supports the following positions of the IoTAA with additional comments as needed:

1. **Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?**

CHOICE supports the IoTAA's recommendation that consumer IoT device manufacturers, developers, importers, and distributors should comply with mandatory cyber security standards. CHOICE also supports a mandatory labelling scheme to promote and highlight adherence to cyber security standards on IoT devices, which retailers should comply with.

2. **Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?**

CHOICE supports the IoTAA's recommendation that the first three principles of ETSI EN 303 645 are included in a minimum baseline for consumer-grade IoT devices sold in Australia. CHOICE

additionally recommends that other principles in ETSI EN 303 645 are considered in the minimum standard, such as ensuring personal data is secure.

3. **What alternative standards, if any, should the Government consider?**

CHOICE supports the IoTAA's recommendation that the Federal Government mutually recognise other standards that are analogous to the principles in ETSI EN 303 645, including the National Institute of Standards and Technology (NIST).

4. **Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?**

CHOICE supports the IoTAA's recommendation to employ the broadest definition of smart devices.

5. **What types of smart devices should not be covered by a mandatory cyber security standard?**

CHOICE believes all smart devices should be covered by basic mandatory cyber security standards. However, as the IoTAA suggests, products may be subject to an equivalent or higher standard than ETSI EN 303 645. This assessment should be made independently.

6. **What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?**

Given the rapid growth in IoT devices, CHOICE believes consumers should be protected with security standards as soon as possible. However, recognising industry may need some time to adjust, we view the IoTAA's recommendation for a 12 month timeframe as a reasonable timeframe, but would be concerned if the timeframe were any longer than this. Additionally, CHOICE recommends adequately resourcing and coordinating education by the Federal Government to encourage business compliance and consumer awareness.

7. **Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for smart devices?**

CHOICE agrees with feedback provided by the IoTAA requesting further clarification on the regulatory framework. CHOICE also notes that the Australian Consumer Law has an existing product safety framework distributing liability between sellers, manufacturers and deemed manufacturers and the ACCC has a monitoring, compliance and enforcement role for these products. We recommend that mandatory cyber security standards for IoT devices be treated in the same way as they are another form of product safety standard.

CHOICE

The Department of Home Affairs and the Federal Government have an opportunity to provide consumers with greater safety and security by implementing mandatory standards on IoT devices. The Department is welcome to contact Rafi Alam ([redacted]) to discuss this submission further.

Yours faithfully,

[redacted]

Rosie Thomas
Campaigns & Communications Director, CHOICE