1 March 2024

Australian Federal Government
Home Affairs
cisgcomms@homeaffairs.gov.au.

To Whom It May Concern,

IoT Alliance Australia submission - 2023-2030 Australian Cyber Security Legislative reforms consultation paper

Internet of Things Alliance Australia (**IoTAA**) thanks the Department of Home Affairs for the opportunity to submit feedback to the 2023-2030 Australian Cyber Security Strategy: Legislative Reforms consultation paper.

The IoTAA is the peak body representing the Australian IoT industry. We encompass the IoT eco-system from IoT service providers, Carriage Service Providers, Industrial IoT *(IIoT ~ industry 4.0)* device manufacturers and users across industry sectors including transport, smart places and infrastructure, food/agribusiness, health and energy.

Internet of Things technologies and resulting "real-time" data practices have, or are in the process of, entering all industry sectors including the fastest growing consumer environments. The immense opportunity for productivity improvement, new business models, sustainability and employment through application of IoT is counterbalanced by the need to build trust with users and to protect lifestyles and the economy. This includes the protection of individuals, companies and critical infrastructure.

We applaud the thrust of the 2023-2030 Australian Cyber Security Legislative reforms as an important step in creating a secure and safe Australia for its citizens and business and a trusted brand for international trade. In particular we strongly support the introduction of minimum security standards for consumer IoT devices.

We look towards further policy initiatives to raise awareness, embed good practice, and increase capability and capacity of users, developers and service providers.

In relation to consumer IoT security we highlight three additional aspects for your attention:

- The need for a voluntary labelling scheme for consumer-grade IoT devices to supplement the introduction of a mandatory minimum standard. This will directly inform consumers of IoT device security and whether device security is at a minimum or higher. Importantly, this market-based approach will encourage and reward leading IoT secure device product vendors in the market.
- The need for well-orchestrated accompanying awareness raising and education program for those affected in the supply chain.
- The wording "Secure-by-design standards for Internet of Things devices" is misleading in that the baseline minimum cannot be considered sufficient as a secure-by-design standard.

The IoTAA would welcome the opportunity to discuss any aspects of our submission in further detail and how the IoT industry may help to achieve a secure, resilient and trusted Australia.

Yours sincerely,

[redacted]

Frank Zeichner

Chief Executive Officer
IoT Alliance Australia
0408 233 762
www.iot.org.au
IoT Alliance Australia

Cyber Security Legislative Reforms Consultation responses

Part 1: New cyber security legislation

Measure 1 - Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

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

Consumer IoT device manufacturers/developers including hardware and software development, importers and local distributers. The retailer could also possibly be responsible if there is a requirement to show a label of some kind.

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?**

Yes. We believe that the first three principles of the ETSI EN 303 645 standard are an appropriate minimum baseline for consumer-grade IoT devices sold in Australia. Especially as it is recognised in other jurisdictions as an appropriate minimum – e.g. UK.

ETSI EN 303 645 has already been adopted in Australia by Standards Australia and was published Nov 17, 2023 and assessed as relevant to the Australian context by the committee (IT-012 Information Systems, Security & Identification Technology).

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

IoTAA encourages the Australian Government to consider other "equivalent" international cybersecurity standards that cover the first three principles of ETSI EN 303 645 to support mutual recognition across the widest market. In particular, consideration of mutual recognition for a NIST equivalent would be good.

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?**

IoTAA supports the broadest definition of smart devices to ensure wide coverage and security coverage for consumers. This UK definition is a good starting point.

We have some concerns regarding the exceptions, e.g. medical devices.

We would suggest requiring a minimum baseline equivalent be incorporated into those parallel mechanisms, so that over time we can be confident that all consumer-grade devices meet the minimum baseline.

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

Consumer IoT products that are covered otherwise by equal or higher minimum standards than the first three principles of the ETSI EN 303 645 standard. For example, this may be the case for classes of medical devices.

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

Once the new standards and compliance legislation is settled, 12 months seems workable for the affected responsible parties to verify and identify complying products for sale in Australia. This assumes there is a well-orchestrated accompanying awareness raising and education program for those affected.

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

It is unclear which elements of the Regulatory Powers Act would apply and be applied. This should be clarified and if considered possibly necessary, carefully in consultation with industry.

The Australian consumer law provides a comprehensive framework distributing liability between sellers, manufacturers and deemed manufacturers. This framework would operate effectively to allocate responsibility where a mandatory standard is applied to IOT products offered for sale in the Australian market.

Measure 2: Further understanding cyber incidents –Ransomware reporting for businesses

Make the reporting as easy as possible.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

17. What should be included in the ‘prescribed cyber security purposes’ for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

If the aim is to ensure that businesses adversely affected by cyber security incidents provide the Australian security directorate with all the information they need, the prescribed cyber security purposes should be limited to purposes related to counter measures against the attacker and protecting the Australian community. There is concern growing amongst the IT community that information provided to the government under its various powers may be used for political purposes and or may embarrass or humiliate an organization that has already suffered as victim of a cyberattack. It is important to limit the use of information provided for the purposes of managing attack strictly for legitimate associated purposes.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident ReviewBoard

20. What should be the purpose and scope of the proposed CIRB?

IoTAA would like to see greater emphasis on lessons learned, feedback and guidance to industry (for broader industry consumption and education) from cyber incident review board. The board will need to have suitable industry representation so the board takes into consideration industry perspectives and needs.

The board could also play a role in analyzing and reporting objectively on the adverse consequences suffered as a result of each cyber attack, including steps, that might be taken to prevent compromised information from being misused in the future.

Part 2: Amendments to the Security of Critical Infrastructure Act 2018

Measure 5: Protecting critical infrastructure–Data storage systems and business critical data

35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

Tightening of the definition of "protected data" to limit the inclusion of data holders and providers that provide "non-essential" data. We believe the data storage provisions need to be clearly focused on business critical data, rather than non-essential data.

As currently drafted the definition discourages regulated entities from providing useful and publicly available information in their reports. The definition of protected information should only cover information that is genuinely confidential and not in the public domain.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

No response to this section

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

The security of critical infrastructure act already provides extensive latitude for the government to share information collected using the act very widely. However, of critical interest to the industry is whether the information collected is used to engage in public comment or debate in relation of particular incident. In our view, Cyber instances should not be politicized on a case by case basis. Regulated entities should be subject to legal obligations and left to deal with public affairs matters without fear that information provided under regulatory powers will be used for political gain.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

No response to this section

Measure 9: Consolidating telecommunication security requirements Telecommunications sector security under the SOCI Act

IoTAA fully supports alignment of telecommunication providers to the same standards as other critical infrastructure entities.

A consideration is what constitutes critical infrastructure within the Telecommunications Act? It is our understanding that public telecommunications providers are in general defined as carriers, by default, under the SOCI Act, unless they are specially exempted – for example, Wi-Fi providers.

Generally IoT service providers should not be regarded as critical infrastructure providers. in most cases, they do not have a sufficiently impactful role in the economy, where one could reasonably regard the service provided as critical. However, there may be particular cases where the Minister may wish to use his or her powers to designate an IT service provider as critical infrastructure, but in general, the approach taken in the existing regulations, where only a service that delivers a standard telephone service, a mobile telephone service or public access to the Internet should be maintained.

About IoT Alliance Australia, (IoTAA)

IoT Alliance Australia (IoTAA) is Australia's peak industry body for the Internet of Things (IoT). This non-profit industry association was established in 2016 to drive a data smart Australia and build a better society and economy through trusted, accessible real-time data powered by IoT technologies.

Our broad membership of over 300 companies work together to drive innovation and adoption though knowledge creation and sharing and building data smart ecosystems, capacity and capability. IoTAA collaborates across key sectors including smart places and infrastructure, food and agribusiness, manufacturing, energy, water, and workforce skills and capability.

IoTAA has three overarching focus areas through which we are delivering high valued projects to our members:

- **Sustainability:** defining and promoting how organisations access the data they need to support their pathway to net zero and circularity.
- **Productivity:** identifying use cases, highlighting industry leaders, codifying good practice and quantifying the value of the adoption of IoT and associated technologies.
- **Trusted technology and data:** creating design and deployment tools and guides and setting the principles and good practices for trust in digital technologies.

For more details, please visit our website https://iot.org.au/