14 April 2023

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

To Whom It May Concern,

IoT Alliance Australia submission - 2023-2030 Australian Cyber Security Strategy Discussion 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 Discussion 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)* and device manufacturers across all industry sectors including transport, smart cities, food/agribusiness, health and energy.

Internet of Things technologies and practices have, or are in the process of, entering all industry sectors as well as 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 critical resources (physical and virtual).

IoT, both consumer and industrial, is of vital economic importance to a sustainable future for Australia. The security of IoT *systems* is essential, not just the end devices, but rather the entire end-to-end solution requires security, including the data generated by, or sent to the IoT devices. The best possible security at end-points is worthless if mid-points in the solution are easily hacked, and vice versa. Similarly, corrupted data can result in incorrect decisions being made where those decisions rely on data from IoT sensors, or in the reverse direction, corrupted instructions can result in harm to industrial processes/systems, and/or consumers, so the integrity of data is equally important.

Further, IoTAA contends that beyond building trust and protection for Australian users, there is an opportunity for Australia to build a "Secure and Safe" brand that will also underpin our reputation as a trusted partner for international trade of physical and virtual resources. We regard that the opportunity of combining government objectives with market-based initiatives will deliver a broader and more rapid impact than pursuing those separately.

In our submission, we have not responded to all the questions posed in the Consultation Paper but rather offer some general observations that will go to many of the points raised in the Paper.

The IoTAA would highlight three key aspects of our consultation response:

- Ensuring consumer IoT security is included in the cyber security strategy, including the implementation of a consumer-informed, industry-led certification and labelling scheme for consumer IoT devices.

- The need for incentives to shift the user (and even service provider) paradigm of "unknown security" to raise the visibility of IoT security credentials, reward secure IoT vendors and service providers, educate and motivate new suppliers to implement security by design and expose bad actors and practices and for users to buy services with easily understood security credentials.

- Facilitating a national register of security accredited suppliers would significantly reduce "re-testing" of suppliers across hundreds (thousands?) of service providers and the risk of multiple testing regimes across state jurisdictions.
- Government should consider only buying from security accredited suppliers. It should also consider assisting Australian vendors and suppliers in achieving security accreditations.

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,

Frank Zeichner

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

IoT Alliance Australia

Cyber Security Strategy Discussion Questions

1. **What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?**

IoTAA's response to the federal government's Strengthening Australia's Cyber Security Regulations and Incentives discussion paper (November 2021) highlighted two significant ideas:

a. The need for incentives to shift the user (and even service provider) paradigm of "unknown security" to raise the visibility of IoT security credentials, reward secure IoT vendors and service providers, educate and motivate new suppliers to implement security by design and expose bad actors and practices and for users to buy services with easily understood security credentials.
b. Ensuring consumer IoT security is included in the cyber security strategy, including the implementation of a consumer-informed, industry-led certification and labelling scheme for consumer IoT devices.

These two above, would complement and strengthen the work being done through the recently updated SOCI regulations.

A critical element is the development of security testing and verification for IoT solutions (devices and the end-to-end system including data integrity), coupled with appropriate labelling schemes that are easily identifiable by consumers and industry.

Security labelling and visibility are fundamental to changing behaviour of users and to drive service provider and vendor incentives. We contend that this is a more wholistic, powerful and faster way to a secure Australia than by penalising bad actors and mandating security requirements onto users, who have poor access to and understanding of security credentials of their suppliers.

It is important that the security accreditation schemes are standards based (preferably international) and that testing be done through *accredited third-party test houses.* Some schemes developed overseas operate on a "self-assessment" framework, where the developer provides their own attestation of the strength of the security they have implemented. While most developers are likely to go through the self-assessment honestly, it will only take a mistake in the self-assessment, or a malicious actor to release an insecure device into the market carrying the certification label, which will quickly break community trust in the label and the scheme. Therefore, it is essential the scheme utilises accredited third-party test houses to test devices, components and end-to-end systems.

Government support to educate the community (both consumer and industry players) is also essential. Awareness of the labelling scheme is vital to create the community "pull" to seek out devices that have been tested and carry the label. Without a strong demand for devices carrying the label, manufacturers and developers will not have the incentive to get their components and solutions tested.

With regards security of **consumer IoT devices – this threat vector could well become the greatest risk** due to the rapidly increasing consumer IoT market (slated to be almost 40% of all IoT devices by 2035). The threat goes far beyond risks for individual consumers, through the risk of "botted" consumer devices which can be marshalled for massive and overwhelming DDOS attacks. **This existential threat is out of the control of operators and owners of Critical Infrastructure and therefore falls directly on governments' responsibility.**

2. **What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?**

Key reforms should be to simplify and where it can be done to avoid and reduce duplicate and overlapping legislative tools. This includes driving a national agenda and avoiding state-based variants. We caution against the introduction of additional regulation, in what is already a complex legislative environment. New legislation, or changes to existing legislation should only be introduced where it will solve a clearly identified problem.

a. **What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?**

Government should consider only buying from security accredited suppliers. It should also consider assisting Australian vendors and suppliers in achieving security accreditations.

Facilitating a national register of security accredited suppliers would significantly reduce "re-testing" of suppliers across hundreds (thousands?) of service providers and the risk of multiple testing regimes across state jurisdictions.

b. **Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?**

The connecting and interconnecting of IoT systems is a (the) major new threat vector to Critical Infrastructure, and indeed all infrastructure and services, including those for consumers. IoT technologies are by definition a system, and not isolated to devices and delivery infrastructure only. It therefore makes sense to take a systems view of security.

c. **Should the obligations of company directors specifically address cyber security risks and consequences?**

Yes

d. **Should Australia consider a Cyber Security Act, and what should this include?**

No comment

e. **How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?**

Facilitating a national register of security accredited suppliers, with transparent labelling for users and consumers would significantly reduce "re-testing" of suppliers across hundreds (thousands?) of service providers and the risk of multiple testing regimes across state jurisdictions.

f. **Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances? i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?**

No Comment

g. Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

No Comment

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

Mutual recognition of security credentials based on international standards.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Identification of bad actors, isolation of insecure service providers and vendors.

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

The role of standards is contemplated several times in the discussion paper, including the role of "best practice" international standards. We consider it important that to the greatest extent possible, international standards are used, especially in relation to IoT security and the testing of IoT devices and solutions. The reason is simple; Australia is a small market globally, and some IoT devices, especially in the consumer space such as smartphones, smartTVs, smart home devices and wearables, can have production runs in the millions globally, well above the volume likely to be sold by that manufacturer in Australia (smartphones is the possible exception). Alternatively, some IoT devices have a price point of only a few dollars, and while it is undeniably important to add security, being able to implement security controls in a consistent manner for devices sold across all international markets can help Australian manufactures defray costs across large global markets. Therefore, alignment with international standards for IoT security is essential, as it will ensure compliance costs are not attributed just to the Australian market.

Australia should strategically consider its "leadership" role in the development, promotion and use of security standards. This is not evidently being done today.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

Government should consider only buying from security accredited suppliers. It should also consider assisting Australian vendors and suppliers in achieving security accreditations.

7. What can government do to improve information sharing with industry on cyber threats?

There is a dearth of understanding of security, related security standards and practices, recognition of secure vendors in industry and especially among consumers. Most information is closely held (almost secretively) by security experts and is poorly translated and disseminated through industry and consumer channels.

There will need to be considerably more awareness raising and education.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve

engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

No Comment

9. **Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?**

No comment

10. **What best practice models are available for automated threat-blocking at scale?**

No comment

11. **Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?**

Yes.

There is a need to uplift cyber skills across the board, from:

- consumers, to
- business users of digital services
- to operators of digital services
- to designers and developers (especially with regards security by design and standards)
- to management in terms of cyber responsibilities and threats
- .

This will necessarily involve training and educational entities and industry engagement to understand the need and obligations.

12. **What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?**

There is a serious gap in IoT and digital skills across Australia, which are vital for the development of the digital economy, the economy and our national productivity. Of these lack of security skills in consistently ranked among the highest needed. E.g. In the IoTAA IoT Skills Barometer, 2020. (We will be launching a new barometer this year).

Mapping of IoT skills and training and that more investment in skills development across the economy is necessary to know where to best place our investment in education, immigration and accreditation.

The Cyber skills Partnership Innovation Fund is a great initiative through which IoTAA is a delivery partner and more investment is evidently needed.

13. **How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?**

No Comment

14. What would an effective post-incident review and consequence management model with industry involve?

One in which learnings are widely shared and inform ongoing practice, awareness and education.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Support the development, implementation, operation and awareness of "secure – by-design" principles.

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

Help small business know who secure vendors and service providers are.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Government should consider only buying from security accredited suppliers. It should also consider assisting Australian vendors and suppliers in achieving security accreditations.

Facilitating a national register of security accredited suppliers would significantly reduce "re-testing" of suppliers across hundreds (thousands?) of service providers and the risk of multiple testing regimes across state jurisdictions.

17. How should we approach future proofing for cyber security technologies out to 2030?

Constant dialogue with and sharing of cyber security risks, standards and practices with industry and users. Government needs to stay informed about security developments and engaged with industry and research that is driving new technologies that can both address security risks and could also open up risks.

Government being involved in developing and being engaged in clear industry driven and accepted standards and accreditation processes that develop responsively over time will also assist future-proofing.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Government should consider only buying from security accredited suppliers. It should also consider assisting Australian vendors and suppliers in achieving security accreditations.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

Work closely with the emerging technology industry (e.g. IoTAA) to share and co-develop good industry security practice.

20. How should government measure its impact in uplifting national cyber resilience?

This is complex. Need to establish a set of metrics that informs community, vendors, service providers to drive good behaviour and good practice.

Beyond the usual measurements of incidents, others may include for example: the percentage of security accredited devices/services sold or in services. The latter could be a forward indicator of cyber reliance.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy

Set understandable, public, measurable targets that include cyber incidents, how quickly and effectively they are managed and responded to, the effectiveness of communication, showing learnings from incidents and demonstrating an understanding of what highly effective looks like with reporting taking place regularly.

Consider an independent body to evaluate government and industry performance against agreed security metrics. This will avoid the evident conflict the government will have in assessing its own performance against security metrics.

About IoT Alliance Australia, (IoTAA)

Who are we?

IoTAA is the peak body for the Internet of Things in Australia. A non-profit industry association, we formed in 2016 to build a better society and economy through trusted, accessible real-time data, powered by Internet of Things technologies. Our broad membership of over 300 companies and 1000 participants collaborate to drive adoption though knowledge creation and sharing, building eco-systems and public advocacy.

Our Vision: A data smart Australia
Our Mission: To advance society through trusted, accessible, automated data.

What is IoT?

The Internet of Things (IoT) is a transformative suite of technologies that, if appropriately and sensitively implemented, can help address the great social and ecological challenges of our time. The Internet of Things encompasses Industrial IoT, which is fundamental to Australia's economy including critical infrastructure, manufacturing, cities and placemaking, construction, productivity and consumer IoT. Consumer IoT is growing exponentially and introducing a seismic shift in data use, trust and the balance in consumer and service provider interactions.

Our need to act

IoTAA's purpose and sense of urgency is driven by Australia's steady decline in global digital competitiveness as recently evidenced by the IMD World Digital Competitive Index where we now rank 20th and 37th for digital training and education respectively.

Our focus

We focus on three areas to achieve the greatest impact for Australia:

- **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 leaders, codifying good practice, IoT/OT convergence and quantifying the value of IoT adoption
- **Trusted technology:** demystifying IoT technology, creating design and deployment tool guides, setting the principles and good practices for trust in IoT and developing an IoT for Good charter.

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