16 September 2020

Australian Federal Government
Department of Home Affairs

To Whom It May Concern,

IoTAA Submission to the Australian Government, Department of Home Affairs – Protecting Critical Infrastructure and Systems of National Significance Consultation Paper – August 2020

Internet of Things Alliance Australia (**IoTAA**) thanks the Department of Home Affairs for the opportunity to submit feedback to the Protecting Critical Infrastructure and Systems of National Significance Consultation Paper – August 2020.

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.

The Alliance supports the principles covered by the recently released 2020 Cyber Security Strategy (6 August 2020), and also the IoT Code of Practice (3 September 2020), and, we welcome the Protecting Critical Infrastructure and Systems of National Significance Consultation Paper.

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).

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:

- The importance of deep intergovernmental and industry engagement and consultation to ensure:
    - Avoidance of duplication of requirements and confusion

    - Alignment of advice, action and understood consequence

- Broaden of the definition Critical Infrastructure to include the security of data

- Providing complementary security at whole economy level to improve security resilience in order to minimise DDoS and other security vectors to Critical Infrastructure and services from the "bottom up".

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

IoTAA Submission re: Protecting Critical Infrastructure and Systems of National Significance consultation paper – August 2020

1. **Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?**

A broad sectoral approach and/or individual entity identification is no longer sufficient when attempting to identify Critical Infrastructure, or organisations of significant national interest, as there are critical components and non-critical components evolving in most sectors – even in defence. There is now a need to define what constitutes critical services, as opposed to entities, as well.

Moreover, some infrastructure may only be critical in rare circumstances, such as selected research facilities. A risk-based approach is therefore required to determine criticality *(i.e. critical levels)* and appropriate mitigation strategies. As in, for example, risk of flooding according 10, 25, 50 or 100-year climate events etc.

2. Do you think current definition of Critical Infrastructure is still fit for purpose?

The definition on page 11 omits the criticality of data assets, as opposed to Information Technologies. This should be explicitly included. Information Security should focus on classifying the information assets that require protection, attributing value to that information, identifying risks to that asset and implementing mitigation strategies for defending against risk to that information, be it data or otherwise, not necessarily the technologies it resides upon.

3. Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

Ensuring the authenticity and validity of data interchanged across supply chains is critical. This includes considering the risks of compromised data sources, poor data management e.g. insufficient metadata to determine validity and authenticity with a resultant inability to detect problems, and poor data sharing policies and processes.

4. What are the common threats you routinely prepare for and those you have faced/experienced as a business?

IoT products and services are not identifiably "secure" or "trustworthy" to buyers and users. The latter purchase and use services based on the history of procurement or recognition of brand, at best. Ensuring good security practices are instituted is vital for most services. IoTAA proposes an industry-based security certification security "Trust Mark" and labelling scheme to address this underlying weakness for all IoT device and service buyers. This assists in the identification of poorly implemented security within devices which are presently being installed and increasing the overall size of threat vectors.

The above could be addressed, only for "Critical Infrastructure" but would still leave interconnected consumers, users and industries vulnerable and does not address cross industry threats.

5. How should criticality be assessed to ensure the most important entities are covered by the framework?

This is a complex question to answer without deep study, particularly as attackers are most likely to pinpoint and target the weakest link in the chain. Therefore, the resilience of the overall security mitigations implemented are only as strong as that lowest protects. Assessment elements must include at a minimum:

- A transparent risk-based approach, to determine criticality *(critical levels?)* and appropriate mitigation strategies are implemented covering all points.

- A cross-sectoral and cross-technology framework, to identify where security risks are important, common or interdependent. To assist this security architecture, the IoTAA has developed the IoT reference framework, covering ten clear levels – enabling resources to discover and document each area within their specific connected ecosystem. And ensure risks and classification are matched with regulatory and good security practice end-to-end. https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf

    - the reference framework has been used as a simple tool in the Water industry and for Energy to identify and position technologies and application of security measures

6. Which entities would you expect to be owners and operators of systems of national significance?

Entities include key companies within the listed Critical Infrastructure industries listed, with the addition of data "owners" throughout the chain.

7. How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?

The TISN must include transparent mechanisms describing how information data is valued, classified and shared.

For example, this could include adopting those identified in the Privacy-Preserving Data Sharing Frameworks edited by the NSW Chief Data Scientist, Ian Oppermann, and is currently in the process of being standardised.
https://www.acs.org.au/insightsandpublications/reports-publications/privacy-preserving-data-sharing-frameworks.html

The Critical Infrastructure Resilience Strategy, should include recognition that the background vulnerability of the whole economy has significant implications for Critical Infrastructure and economies. For example, loss of availability through DDoS attacks. As such, IoTAA recommends that the industry-driven IoT Security Trust Mark certification and labelling scheme be adopted enabling procurement agents across industries and government to select known, independently evaluated, claims tested, trusted devices for deployment. This clearly strengthens and supports the visibility and demonstrates real-world application of the Federal Government's recently published Voluntary Code of Practice for IoT Security.

8. What might this new TISN model look like, and what entities should be included?

This needs a deal of consultation and cross-industry and government analysis.

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

Government should ensure to the maximum extent possible that the principles and models do not introduce redundant overlay requirements. That is, where existing legislation covers requirements in a particular sector, that these equivalents are recognised and not rewritten and cause unneeded additional expense for no gain in actual security. Self-regulation should be encouraged and supported by Government providing critical sectors ensure appropriate checks and balances are implemented to deliver satisfactory assurance that mitigation strategies to address identified risks are current and effective.

10. Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

The principles do not adequately identify the need for good data information security assurance practice, integrity checks, access controls and data policies and currently focus on traditional technologies and physical infrastructure. Taking a legacy security approach to emerging data systems will expose critical infrastructure to significant risks.

11. Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

It is critically important to clearly establish essential criteria in the legislation, at a specific level, against which any measures contemplated in subordinate instruments of regulation, industry codes, standards, guidelines etc. can be developed and most importantly measured to demonstrate evolving maturity over time.

Such criteria should include

- the necessity of the measure;
- its proportionality, including in relation to any attendant costs of the measure;
- its effectiveness;
- its technical feasibility;
- the legitimate interests of the critical infrastructure entity;
- the availability of other means to achieve the desired outcome;
- the cost is commensurate with the value gained and the risk mitigated;
- the intrusiveness of the measure, any implications for privacy and whether less intrusive measures could be equally effective; and

the need for a regular review as to whether the criteria remains appropriate.

Care needs to be taken to ensure the cost of securing against a prospective threat is in line with the value of the loss should the threat be realised. For example, requiring high levels of encryption on the data from an ambient temperature sensor may not be justified, whereas the ability to patch security flaws preventing an IoT device being co-opted into a botnet will help prevent attacks where the device owner may not be the victim. Without clearly documented baselines, metrics and regular measures and reporting of value in place the maturity of the security measures implemented cannot be quantified.

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

We have not canvassed members regarding whether they operate in-line with the principles, anecdotally however the response, at best, would be partially. For some, this likely would require significant training, culture change, new processes, and also changes to underlying technologies and even new technologies – which they would consider costly.

13. What costs would organisations take on to meet these new obligations?

See answer to question 12 above.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

The telecommunications sector already has substantial security requirements in place, which largely fall in-line with the principles. Please refer to the consultation submission from Communications Alliance.

Considering the potential effects of attacks that may indirectly affect Critical Infrastructure, for example disruption through attacks across common devices there is value in ensuring implementation of separate core network elements. This would however require significant additional costs, including additional transmission capacity and interoperability assurances.

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?

There is a significant risk that if the legislation is not carefully written in close consultation with each industry across the many affected sectors, duplication of existing oversight requirements will occur, particularly when considering the effects of emerging technologies and critical information data processing and handling systems as it is decentralised. The risk of redundant and legacy legislation is real, specifically policy is required to move as rapidly as the technologies themselves.

Please also note the answer to question 17.

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

There should be a considered engagement and consultation process in developing the guidance for sector regulators to minimise redundancy and to clarify roles and responsibilities, an emphasis should be placed on industries clearly demonstrating capacity to develop and self-regulate where possible.

Ideally a set of understood, requirements at differing levels of "industry criticality" might be applied to identify common attributes for all (most industries), complemented with sector specific requirements, as needed. The ability to clearly document and demonstrate confidence in assurance through compliance with industry self-regulation is an important aspect government should consider.

17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

This is difficult to answer over the many sectors covered by our associations remit *(at least ten)*, however some observations are relevant in general:

- the various sectors have regulators that are often fragmented in responsibility, particularly between Federal and State
- It is likely the above have differing understandings and responsibilities for security in their sectors
- These regulators are likely, in the first instance, to have a better handle on how to interpret levels of criticality for security purposes, based on criteria set by the TISN and other centralised tools – however will need to be brought up to parity in relation to these requirements
- That an overlay security mechanism across all "critical" infrastructure needs to interoperate with, and indeed across, the existing industry regulatory frameworks in a way which minimises rework, contradiction and possible confusion through ambiguity.

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

- Clear and agreed definitions for various levels of Critical Infrastructure, derived from taking a risk based approach and assessments applied across physical infrastructure and specifically information data sets
- Clear metrics, measurement and assessment of effect of application of differing criticality levels and mitigation costs vs value
- Consistent, regular engagement with industry stakeholders to understand degree of complexity, time and costs to implement
- Determination of best course of action/prioritisation for each sector plus management of consequential follow-on costs to users and citizens
- Regular communication programs to explain measured benefits/costs and value to stakeholders.

19. How can Government better support critical infrastructure in managing their security risks?

Providing clear consistent and regular situational awareness regarding identified threats vs risks would be valuable.

20. In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

21. Do you have any other comments you would like to make regarding the PSO?

22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?

The following clarifications would be beneficial to the IoT industry:

- Clear and transparent criteria for determining levels of critical services (as opposed to industries)
- An understanding of the flow-on consequences of applying mitigation actions across critical services (especially in relation to end users e.g. higher prices, greater surveillance, restricted services etc) to assist communications and determining where the cost burden should fall, or be shared.
- Clearly documented success factors, current baseline metrics (where we are now) and the measurements vs investment by Government to target strategic objectives and regular reporting to ensure, firstly advancement and maturity in securing resilience and, secondly value in achieving the success.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

The IoTAA is introducing an industry-led IoT products and services security certification and labelling scheme to Australia. The IoTAA could provide advice on which vendors have passed their security claim testing and been evaluated against the Baseline Requirements such as those contained in the Australian IoT Code of Practice. This would assist government, Critical Infrastructure and organisations of national significance in making procurement decisions about which vendors' products should be preferred.

The certification and labelling scheme is funded voluntarily by industry, with no government outlay required. Impact on end-users is minimal form a price point of view, however invaluable in terms of knowing which vendors have had their products/services security claims independently and rigorously verified.

25.What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

26.What are the barriers to owners and operators acting on information alerts from Government?

The following barriers are pertinent to the IoT industry:

- lack of internal security skills, policies, processes and culture
- lack of understood framework and processes for interaction between government and owners and operators. There are many "silos" within Federal and State government departments and agencies with a variety of remit across the security "sphere". In our experience, this leads to confusion as to the agency responsible for each type of risk/threat.
- funding allocation to implement changes to address the above

27.What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

Clearly defined responsibilities and the resulting consequences of actions, or in-action, on users, and service providers.

Any included security obligations require clearly understood, mutually agreed consequences, regular review/revision (for currency/applicability) and clear communication.

28. What safeguards or assurances would you expect to see for information provided to Government?

Confidentiality of personal and corporate information, to all but a limited set of trusted individuals under agreed circumstances.

29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

Without a better, and clearer, explanation and understanding as to what such powers entail and how those would be translated into regulation IoTAA highlight the inherent risks that may be attendant to a direct action power.

The Consultation Paper notes; *"Government's unique understanding of Australia's threat environment and the interdependencies within critical infrastructure sectors [which] position it best [to] determine appropriate preventative actions and resource allocation in a crisis."1 The Paper also highlights Government's role "to use its enhanced threat picture and unique capabilities to take direct action to protect a critical infrastructure entity or system in the national interest."2*

We would question the above assertion and note that any direct action should be well identified and agreed in the aforementioned Playbook(s) so that consequences and capability (across governments and industry) are mutually agreed and aligned.

30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

31. Who should oversee the Government's use of these powers?

32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?

35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

---

[1] *p. 28, Department of Home Affairs, Protecting Critical Infrastructure and Systems of National Significance, Consultation Paper, August 2020*

[2] *p. 29, ibid*

36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

About IoT Alliance Australia, (IoTAA)

IoTAA is the peak industry body representing IoT in Australia. Over 500 participating organisations and 1000 individual participants are working to accelerate the adoption of IoT across the Australian economy and society.

IoTAA's purpose is creating and developing sectoral IoT advancement and alignment with key sectors, including through Government Industry Growth Centre activities, Infrastructure Australia, state governments and key sectoral bodies with an initial focus on water and energy resource management, food and agribusiness, transport and smart cities.

IoTAA's Terms of Reference

- Providing an IoT strategy and policy recommendations with focus sectors to align with government and industry priority areas.
- Engage and collaborate with key stakeholders including major sector aligned growth centres, industry associations, major government influencers
- Align IoT solutions to meet the needs of industry and consumers
- Create more IoT awareness, engagement and education for consumers, markets, and governments.
- Apply the learnings of global best practice sector initiatives such as the US Smart Cities IoT initiative.

IoTAA's work-program spans 12 work-streams which focus on industry vertical sectors and key IoT enablers. They are:

Sectoral Focus

1. Smart Cities
2. Food and Agribusiness
3. Water
4. Energy
5. Transport
6. Manufacturing
7. Health

IoT Enablers

1. Collaboration
2. Data Use, Availability and Privacy
3. Cyber security and Network Resilience
4. Platforms and Interoperability
5. IoT Start-ups

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