IoTAA submission to:

Department of Home Affairs consultation on:

Australia's 2020 Cyber Security Strategy

1 November 2019

Contents

Executive Summary

The IoT Alliance Australia (IoTAA) welcomes the opportunity to provide a submission to the Department of Home Affairs call for views on *Australia's 2020 Cyber Security Strategy*.

We are in the early stages of the fourth industrial revolution, and the Internet of Things (IoT) is already playing a pivotal role in enabling the revolution by bridging the gap between the physical and digital worlds. IoT is fundamental to the future evolution of our economy, and as the scale and scope of IoT increases, both in number of devices and the complexity of the data fabric that sits at the core of an IoT enabled economy, so too the cyber-attack risk grows.

Our submission draws on the industry approach documented in the IoTAA's 2017 **Strategic Plan to Strengthen IoT Security in Australia**[1], and focuses on the full end-to-end IoT services and solutions "eco-system", not just IoT devices (as IoT is commonly thought of). Any IoT eco-system can be defined by the **IoT Reference Framework**[2] which has been developed by the IoTAA cyber security and network resilience work-stream.

We propose the best way to strengthen IoT security in Australia is through the deployment of a Security Trust Mark (STM) scheme to provide consumers and businesses confidence that the devices and solutions they are purchasing to deploy in their IoT ecosystem meet the vendor's claims of its security capabilities. While there are moves in the United States and the United Kingdom to introduce voluntary accreditation schemes into law, we do not recommend mandating schemes through legislation.

The STM scheme we propose is an industry led initiative which uses market signals and responses to drive vendor and user behaviour (e.g. somewhat like the ANCAP or Energy Rating marks). It provides a compelling commercial incentive for vendors, practitioner and users to ensure good IoT security practices. Customer awareness of the scheme drives demand for IoT products and services to carry the Security Trust Mark, which in turn, drives suppliers to voluntarily meet the requirements to obtain the right to carry the Security Trust Mark.

Our submission provides a brief summary of the assessment and gap analysis we have conducted on a range of guidelines and schemes proposed by a range of entities internationally, and explains why we recommend the IoTAA's STM scheme as a key pillar in any strategy to strengthen IoT security, and hence cyber security, in Australia.

[1] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Strategic-Plan-to-Strengthen-IoT-Security-in-Australia-v4.pdf
[2] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf

Introduction

The IoT Alliance Australia (IoTAA) welcomes the opportunity to provide a submission to the Department of Home Affairs call for views on *Australia's 2020 Cyber Security Strategy*. As the discussion paper observes, cyber security has never been more important to Australia's economic prosperity and national security. The discussion paper solicits views on a wide range of topics under the cyber security umbrella, and as Australia's peak industry body for IoT, we are pleased to be able to provide our direction and views on cyber security as it relates to IoT; from the security of end devices and networks through to the entire eco-system of the businesses and government entities that use and rely on the data they generate.

Our submission is in three parts:

- Firstly, we provide background on the importance of IoT in the context of the fourth industrial revolution;
- We then outline our proposed approach for securing the Internet of Things commencing with a review of guidelines and schemes internationally;
- Finally, in the appendix, we provide answers to a number of the direct questions in the discussion paper.

About IoT Alliance Australia (IoTAA)

IoTAA, www.iot.org.au, is a not-for-profit industry association incorporated in July 2016. We are the peak Australian IoT industry body. The vision of IoTAA is:

> **"To empower industry and society by accelerating IoT innovation and adoption for Australian economic and societal benefit."**

We see ourselves as a prime instigator of IoT collaboration and advancement in Australia through a network which includes community and citizens, government, research and industry – all of whom contribute to our work.

IoTAA now has over 500 organisation members and 1000 participants. IoTAA runs twelve programs (workstreams) covering:

- Industry sectors:
  - Transport;
  - Cities;
  - Manufacturing;
  - Water;
  - Energy;
  - Health;
  - Food and Agribusiness;
- Collaboration;
- Data use, access and privacy;
- Cyber security and network resilience;
- IoT start-up innovation; and
- Platforms and Interoperability.

Internet of Things, the Fourth Industrial Revolution and Security

It is commonly recognised we are now entering the era of the Fourth Industrial Revolution. Professor Klaus Schwab, founder and executive chairman of the World Economic Forum (WEF) published his book "The Fourth Industrial Revolution"[3] in 2017 where he outlined a range of megatrends that will, and already are, fundamentally changing the way we live, work and relate to one another. Key amongst the megatrends driving this revolution is the Internet of Things (IoT), which is described as one of the main bridges between the physical and digital.[4] IoT enables us to capture data from a massive array of physical world scenarios for processing in the digital world, allowing us to make more informed and accurate decisions in quicker timeframes to reduce cost, improve performance and reduce our environmental impact. In short, IoT is a key enabler of the fourth industrial revolution, making it a fundamental requirement for the future evolution of our economy.

IoT has already entered every facet of our lives, from medical/health devices and wearables to industrial and manufacturing control systems, agriculture, transport, smart cities and smart homes. Cyber-attacks on these devices and systems can take many forms from stealing data (which in some cases includes personal, private information), or disrupting control systems through to co-opting devices to participate in bot armies.

IoT security is far more than concerns about privacy, or disruption to our lives; it goes to the very core of our sense of personal security. To illustrate, a recent opinion piece[5] in the California Mercury News describes the sickening and helpless feelings of the author as a hacker, having infiltrated a home security camera uses the internal speaker to threaten to steal an 18-month baby from the author's home. Once privacy and security is invaded to this level, it is extremely hard to regain the trust; trust that underpins the digital world and the benefits our society derives from it.

As the number of IoT devices grows exponentially, so too does the potential security attack surface[6]. And, as our reliance on that data for our economic competitiveness and for monitoring and controlling our environmental impact grows, so too does the need to ensure the devices, and the delivery of the data generated by the devices is protected and secure.

Now more than ever, cyber security is of critical importance, as the discussion paper notes. A greater emphasis on building in good security practices and a transparent method for identifying secure IoT components and services is essential, and fundamental to a national Cyber Security Strategy.

[3] https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab
[4] The Fourth Industrial Revolution, Klaus Schwab. Section 2.1.2.
[5] Opinion: The voice from our Nest camera threatened to steal our baby. The Mercury News, 18 October, 2019. https://www.mercurynews.com/2019/10/18/the-voice-from-our-nest-camera-threatened-to-steal-our-baby/
[6] Attack Surface: https://en.wikipedia.org/wiki/Attack_surface

Securing the Internet of Things

IoT Security – IoTAA's definition

We believe that IoT security moves beyond the traditional three pillar ICT cyber security model of "confidentiality, integrity and availability" (the CIA model) and is categorised as the preservation of:

a. **Confidentiality** - The property that information is not made available or disclosed to unauthorised individuals, entities, or processes;
b. **Integrity** - The property of safeguarding the accuracy and completeness of assets;
c. **Availability** - The property of being accessible and usable upon demand by an authorised entity;
d. **Safety** – The property of being able to be used without harm to a person or persons;
e. **Resilience** – The property of being able to sustain continuous operation even when under attack.

Any or all of these aspects may be of importance in a particular IoT use case.

Five Eyes (FVEY) Statement of Intent regarding the security of the Internet of Things

On 23 October 2019 FVEY released a **Statement of Intent regarding the security of the Internet of Things**[7] that expects industry to develop IoT devices following security by design principles and that the Five Eyes partner nations agree to:

1) Collaborate with respective industry and standards bodies to provide better protection to users by advocating that devices should be secured by design.
2) Actively seek out opportunities to enhance trust and raise awareness of security safeguards associated with IoT devices in our respective nations.
    a. Identify and engage industry partners who share Five Eyes' goals to enhance the security of IoT.
    b. Identify and engage likeminded nations to encourage international alignment on IoT security, unlocking innovation that builds a strong economy that works for everyone.
3) Share information with Five Eyes partners in a timely manner through appropriate channels and arrangements, consistent with international and domestic law, to aid in the overall improvement of IoT security.

The IoTAA is very encouraged by the Five Eyes nations committing to work collaboratively with industry and standards bodies to address the risks posed by insecure devices and networks, and we would welcome the opportunity to work with the security agencies of the Five Eyes nations to strengthen IoT security.

[7] https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

IoTAA Strategic Plan to Strengthen Security

In September 2017, the IoTAA released version 4 of its **Strategic Plan to Strengthen IoT Security in Australia**. The plan outlines eight key items and describes proposed policy, stakeholders and steps required to implement them. Four of the eight were identified for priority focus, and while good progress has been made, more remains to be done.

The second of the eight key items, and the one we focus on here, is to:

> **Develop, implement and promote an IoT product security certification program: an independent IoT product security claims-testing, evaluation and certification "Trust Mark" program for demand-side assurance.**

Importantly, it is not just about the individual IoT devices; it is the full end-to-end solution that requires security consideration. Each IoT deployment is unique and can be quite diverse. Take a smart city as an example. It would be impossible to define a traditional IT security architecture for such an environment given the complex array of scenarios under the smart city umbrella. Smart cities embrace everything from environmental monitoring (air and water quality), smart solutions to reduce energy consumption (smart streetlights and monitors to detect when bins need emptying), to transport, road and parking monitoring. Each of these individual scenarios can be ecosystems in their own right, with separate networks and platforms implementing individual scenarios.

That's why we have developed and released the **IoTAA Reference Framework**[8] and **Application Guide**[9] – so IoT practitioners, vendors, solution designers, businesses and even consumers could see all the layers where security, privacy and safety need to be considered. Users of the framework can build a model of their ecosystem and wrap governance, risk, compliance and regulatory requirements around it, so that each element of the IoT ecosystem can be viewed from the perspective of any of the stakeholders.

In addition to the Reference Framework, we have completed the design for the **Security Trust Mark (STM) scheme**, and it is ready for the education, distribution and implementation phases. The STM is an industry led initiative which uses market signals and responses to drive vendor and user behaviour (e.g. somewhat like the ANCAP or Energy Rating marks).

More detail on the scheme is in the section below titled IoTAA's Security Trust Mark (STM) Scheme. But firstly, a review of the landscape of security guidelines and schemes.

Review of international IoT security guidelines and schemes

This section of our submission provides a short survey of the global landscape of IoT guidelines and schemes designed to improve security. These schemes have been quick-to-market, and serve a useful purpose in that their early establishment has provided IoT practitioners and vendors a base to start from.

[8] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf
[9] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-Application-Guide-v1.0.pdf

Guidelines

A number of industry groups, including the IoTAA, have produced guideline documents to assist practitioners, vendors and users understand good practices for IoT security. Examples of IoT security guidelines include:

- IoTAA's **Internet of Things Security Guideline**[10] which provides thirty mandatory requirements and seven recommended practices;
- National Institute of Standards and Technology (NIST) **Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks**[11] which uses an iterative lifecycle management approach to identify and develop risk mitigation strategies on three key areas of device security, data security and the protection of personal information;
- The GSM Association's (GSMA's) **IoT Security Guidelines and Assessment**[12], which includes 85 detailed recommendations for the secure design, development and deployment of IoT services;
- The UK's Department of Digital, Culture, Media & Sport's (Dept DCMS's) **Code of Practice for Consumer IoT**[13], which links to ETSI standard TS 103 645 titled Cyber Security for Consumer IoT with 13 top-level provisions for IoT security.
- The European Union Agency for Cybersecurity (ENISA), **Baseline Security Recommendations for IoT**[14], Aims to set the scene for IoT security in Europe, serving as a reference point in this field.

All of these guidelines serve a very useful purpose in that they enable vendors to consider the security features they should implement, and they allow users and practitioners to ask questions of vendors and solutions providers to self-test whether they believe the services and solutions they have meet their expectations of sufficient security.

However, because these guidelines are often high level descriptions, they don't facilitate a mature conversation about what this actually means, or what constitutes a good quality implementation, and users of the guide(s) who don't possess detailed security knowledge can be left wondering whether actions and implementation of IoT security is sufficient.

Assessment and accreditation schemes

In addition to guideline documents, globally a number of assessment schemes have emerged. These take the guidelines discussed in the previous section, or a variant thereof, and define a scheme for assessing the extent to which security has been implemented. Like our STM scheme, these schemes are all voluntary, in that there is no mandated or legislated requirement for IoT vendors, practitioners or users to have their devices/solutions tested. Unlike our STM scheme, many of the

[10] IoTAA. **Internet of Things Security Guideline**, Ver 1.2, Nov 2017. http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

[11] NIST. Internal Report 8228 (IR8228), **Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks**, June 2019. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

[12] GSMA. **IoT Security Guidelines and Assessment**. Ver 2.1, March 2019. https://www.gsma.com/iot/iot-security/iot-security-guidelines/

[13] UK DCMS. **Code of Practice for Consumer IoT**. June 2019. https://www.gov.uk/government/collections/secure-by-design

[14] ENISA. **Baseline Security Recommendations for IoT.** November 2017. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

schemes operate on a self-assessment basis where the user or practitioner conducts their own assessment.

Some examples of assessment schemes include:

- IoT Security Foundation's (IoTSF's) **Best Practice User Mark**[15], is a voluntary certification scheme that assesses the entire supply chain and allows organisations following the IoTSF's Security Compliance Framework to use their Best Practice User Mark. Security can be self-assessed, or use an accredited third party.
- Industrial Internet Consortium's (IIC's) **Security Maturity Model**[16]. The scheme uses an Agile-style of methodology (called Plan-Do-Check-Act) to iterate towards a desired security "goal-state". This embraces a 'fit-for-purpose' approach to security, allowing practitioners to decide a level of security appropriate to the scenario and risk. By identifying both the current and desired maturity status, vendors can work to close the gap. An ongoing 'persistent maturity status' can be maintained by the same approach. The scheme is self-assessment only, and does not offer a trust-mark.
- International Electrotechnical Commission's (IEC's) **Security for Industrial Automation and Control Systems**[17] is a security standard for Industrial Automation and Control Systems (IACS). Manufacturers (etc.) can have their product development processes certified by an accredited IEC 62443 certifier.
- Underwriters Laboratories' (UL's) **IoT Security Rating**[18] which is an evaluation process that assesses critical security aspects of smart products against common attack methodologies and known IoT vulnerabilities.

Should IoT security be mandated?

An important question to ask at this point, given the guidelines and schemes we have reviewed, is whether there is benefit in mandating the use of guidelines or assessment schemes to improve IoT security.

We are aware of jurisdictions that have, or are moving toward mandating the implementation of security features and/or practices. In September 2018, California enacted legislation[19] such that from 1 January 2020 manufacturers of a connected device are required to equip the device with reasonable security feature(s), appropriate to the nature and function of the device. Similarly, the Internet of Things (IoT) Cybersecurity Improvement Act of 2019[20] introduced into the US Senate in March 2019, if passed, would require IoT-related devices procured by the U.S. government meet certain minimum security criteria, although this Bill does not extend to consumer equipment.

Mandating of fixed security requirements using approaches such as these can be controversial. Critics[21] of mandated approaches note that if the threshold is set too low, it results in a false sense of security. Of course the converse can be true of mandated schemes as well. Setting the bar too high in terms of either the number of mandated security features and/or the threshold of the features

15 IoTSF. **Best Practice User Mark**. December 2018. https://www.iotsecurityfoundation.org/best-practice-user-mark/
16 IIC. **IoT Security Maturity Model**. February 2019. https://www.iiconsortium.org/smm.htm
17 IEC. **Security for Industrial Automation and Control Systems**. TS 62443-1. July 2009. https://webstore.iec.ch/publication/7029
18 UL. **IoT Security Rating**. https://ims.ul.com/IoT-security-rating
19 https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327
20 https://www.congress.gov/bill/116th-congress/senate-bill/734
21 https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XbN5_5IvPIV

results in inflexibility that restricts the ability to implement fit-for-purpose security features without burdening manufacturers with security feature costs that are not proportionate to the risk. We are not in favour of mandating or legislating prescriptive security approaches for these reasons.

A step down from prescriptively mandating specific security features is mandating the introduction of voluntary certification schemes. Globally, some jurisdictions are looking at this approach. In Europe, the EU Cybersecurity Act of April 2019[22] tasks ENISA with the establishment and ongoing maintenance of an EU-wide cybersecurity certification framework[23] for ICT products, services and processes. The European Commission claims companies doing business in the EU will benefit from only having to certify their ICT products, processes and services once, as their certificates will be recognised across the European Union.

Similarly, the Canadian Multi-stakeholder Process has as the first two of the recommendations in its Final outcomes and recommendations report[24] to: 1) Develop a security label for Internet of Things (IoT) and other digital products; and 2) Adopt standards for testing and evaluation of IoT products to assist purchasing decision. In the US, the recent reintroduction of a 2017 Bill titled the Cyber Shield Act[25] would see the formation of an advisory committee to establish a voluntary accreditation scheme.

Voluntary accreditation schemes provide compelling commercial incentives for suppliers to participate when consumers and businesses actively seek products carrying the label. Increased vendor participation will then raise further awareness amongst the wider community, creating a virtuous circle that raises awareness and security.

While there is merit in a legislated/mandated self-certified accreditation schemes in terms of getting the scheme 'off-the-ground', our view is that it must be an industry managed scheme rather than a government owned and operated scheme. Governments come and go, and so too does funding and resourcing to run schemes such as security certification. For reasons of longevity, it is vital any scheme is ultimately owned and operated by industry, rather than by government.

IoTAA's Security Trust Mark (STM) Scheme

The IoTAA's Security Trust Mark (STM) scheme is a transparent and accredited industry operated scheme that is critical to Australia's cyber security. In developing the STM scheme, IoTAA has engaged with Government and has welcomed feedback and input over recent years.

The objective of the STM scheme is to meet the needs of government and industry for cost effective and efficient functionality claims testing of the security of IoT devices or services. The STM scheme is aimed primarily at IoT devices and services to meet information assurance requirements at the higher impact levels, for purchase by central government and the wider public sector, particularly in the areas of transport, health, agricultural, industrial control systems, and smart cities.

While the certification program itself is ultimately self-funding, financial assistance will be required for the next phases required to launch, administer and market the scheme; and to maintain and update the scheme as IoT and technologies evolve. The STM scheme is industry developed, and to

[22] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[23] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[24] https://iotsecurity2018.ca/draft-outcomes-report/
[25] https://www.markey.senate.gov/imo/media/doc/Cyber%20Shield%202019.pdf

date, has relied on the good-will of volunteers, albeit experts in their fields, donating their time and effort to build the program.

Our thesis is that through the STM scheme, government, industry and the community will contribute to building a more resilient and secure national IoT infrastructure. This will be achieved by consumers, businesses and government having access to, and confidence in STM evaluated products; enabling them to ascertain which vendors and products are currently certified and their status at any given time. This in turn sends a strong signal to vendors of IoT products and services to build in security into their products and practices, and to advertise their security compliance as a competitive advantage.

The government, in taking the lead in prioritising procurement for STM accredited products and services would provide a powerful catalysing effect in encouraging and assisting industry adopt and demonstrate good IoT security practice.

Key elements of our scheme that differentiate from other schemes:

- Verification is against the **vendor's security claims**, with a minimum baseline required set (i.e. either legislated such as in California – although, we recommend against this - or baseline defined by organisations such as ENISA). This overcomes a 'one-size-fits-all' approach to IoT security, while still maintaining a minimum security baseline. It also allows for different testing at the different layers in the Reference Framework covering any IoT device.
- A Decision Authority (DA) oversees the scheme, including administration, the accreditation of the test facilities (ATFs), technical oversight, review of Initial Claims Documents (ICDs), review of ATF letter of recommendations, the issuance of certifications and the publication of the Evaluated Products List (EPL).
- Testing under the scheme is performed by a **third-party** Accredited Test Facility (ATF) engaged by the vendor. This is an important differentiator compared to other certification schemes which operate on the basis of self-assessment and compliance.
- The vendor and the ATF jointly work to develop an ICD which includes details about the product seeking certification, the vendor's security claims and a draft testing methodology. This ICD is then submitted to the DA for review and approval.
- Once the ICD is approved the ATF executes the evaluation and, within 30-days, provides to the DA a full test report, a summary test report and a letter of recommendation.
- The DA reviews the documents and decides on a fail or pass and issuance of a certification.
- Once certified the vendor's product, firmware and any other relevant particulars are published on the EPL along with the summary test report.

Security is an ever moving target, and a product that meets its security claims one day may be vulnerable the next. Therefore, the STM scheme has been designed to ensure there is a mechanism in the certification baseline that vendors have for mandatory notification of vulnerabilities. In our STM scheme, once the DA is aware there is a vulnerability, i.e. reported via a source such as a Cyber Emergency Response Team (CERT) alert, the vendor will be contacted and their product certification will be placed into a suspended status until the vulnerability has been addressed and the product regressively tested and verified by the vendors' ATF and a letter issued to the DA by the ATF confirming this.

Education and Awareness

The final component required to improve security for the Internet of Things is education and awareness. The cyber security work-stream of the IoTAA is also working on delivering IoT security awareness guides for stakeholders, including the supply-side (manufacturers, developers and suppliers) as well as the demand-side (consumers, procurement departments and agencies). On the one hand encouraging and providing resources for secure IoT by design, safety by design and privacy principles, and on the other hand empowering consumers and procurement agents with the security, safety and privacy questions they need to be aware of when approaching the market for IoT products and services. These guidelines will play an important role in raising awareness of the need for good IoT security practices.

Conclusion

Commensurate with our **Strategic Plan to Strengthen IoT Security in Australia**, we propose the introduction of our STM scheme is the best way to strengthen IoT security in Australia. The STM scheme we propose is an industry led initiative which will provide consumers and businesses confidence in the devices and solutions they are purchasing and provides a compelling commercial incentive for vendors and practitioner to ensure good IoT security practice.

Appendix 1: Answers to selected consultation questions

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

Having legislative frameworks in place that recognise the fundamental importance of the internet and digital systems to the Australian economy are of prime importance, and as such government in its role as legislator should engage industry to ensure the legislative framework is modernised appropriately.

Furthermore, government should take an active role in assisting industry to manage IoT security. This could take the form of:

- support from government for the Security Trust Mark (STM) scheme;
- the procurement of STM products; and
- education of the public, businesses and institutions, around best and appropriate practises to being cyber secure, including purchasing STM marked products.

5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

Voluntary accreditation/certification schemes have great potential to improve trust within the community of IoT users. In the body of our submission, we reviewed initiatives in the European Union and the United States that introduce voluntary accreditation schemes. We are supportive of such initiatives, and we recommend commercial incentives provide a more compelling approach for suppliers to participate in such schemes.

Government support for any accreditation/certification scheme should take the form of procurement policies that require government to purchase devices and solutions that carry the certification.

6. What customer protections should apply to the security of cyber goods and services?

In the context of IoT, the STM scheme would enable consumers and businesses to purchase IoT devices and solutions with confidence. This could form the cornerstone of customer protection(s) for IoT. Including assurance that the vendor's security claims have been independently validated and that the certified products listed on the evaluated products list are current and can be trusted by customers.

7. What role can Government and industry play in supporting the cyber security of consumers?

Government backing of industry initiatives such as the IoT Reference Framework and the Security Trust Mark scheme through endorsement and financial support. For organisations like the IoTAA these programs have been delivered to date by industry volunteers, however require funding to deliver the administration and marketing of these bodies of work.

Support of the Awareness and Education material that industry organisations such as the IoTAA are creating that provide resources in the form of guides to both the demand side (consumers/procurement agents), empowering this audience with knowledge of potential cyber security risks that exist in IoT and equipping them with straight forward techniques to avoid or minimise these and providing some key questions that they need to ask of their vendors and suppliers at the point of purchase/evaluation. On the other hand IoTAA security awareness guide material for the supply side (manufacturers/developers/suppliers/distributors/retailers) the material addresses good practice such as building in security by design, safety by design principles and good practice privacy for data.

8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

Industry can increase the security, quality and effectiveness of cyber security and digital offerings by adopting and supporting the Security Trust Mark (STM) scheme. As vendors and manufacturers promote product that have obtained the Trust Mark, consumers and procurement staff will become more aware of the scheme, and will deliberately seek out IoT products and services that carry the Trust Mark, thereby providing incentives for more vendors and manufacturers to participate in the scheme.

For instance, the IoT Reference Framework and Application Guide, which map IoT systems using a layered approach, enables IoT users and other IoT practitioners full visibility of the IoT ecosystem. Government assistance in providing a simplified version of the document, suitable for the Australian public would assist in developing an appreciation for the STM on all IoT product sold in Australia.

Further details of the STM scheme, the IoT Reference Framework and Application Guide are contained in the body of our submission.

9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?

In the Security Trust Mark (STM) scheme we have described is an industry operated scheme. From the government's perspective, the most obvious benefit of an industry-run scheme is avoiding having to develop and operate its own scheme. The scheme gives oversight to government, via the inbuilt reporting mechanisms for the number of devices, platforms and services that have obtained the Trust Mark, and the mandate to notify the Decision Authority of any identified vulnerabilities. Further details of reporting, including reporting of breaches, is contained in the body of our submission.

10. Is the regulatory environment for cyber security appropriate? Why or why not?

The body of our submission contains a number of examples where jurisdictions internationally have either legislated, or are in the process of creating legislation to improve cybersecurity. Some of these are examples where government is attempting to mandate minimum security requirements for IoT devices through legislation. Our view is this can lead to unintended consequences. If the threshold is

set too low, devices and solutions easily pass the requirements but may be vulnerable to attacks, leading purchasers into a false sense of security. Conversely setting the bar too high in terms of either the number of mandated security features and/or the threshold of the features results in inflexibility that restricts the ability to implement fit-for-purpose security features without burdening manufacturers with security feature costs that are not proportionate to the risk. As such, we are not in favour of mandating or legislating prescriptive security approaches, and advise against such approaches.

Our proposal to improve security for IoT is through the introduction of a voluntary accreditation scheme, as it allows for fit-for-purpose security features that in the case of the STM scheme we have designed, are independently tested by an accredited third-party test facility.

While there is merit in legislating for the introduction of a voluntary accreditation scheme to get the scheme 'off-the-ground', our view is that it must be ultimately be an industry managed scheme rather than a government owned and operated scheme. Governments come and go, and so too does funding and resourcing to run schemes such as security certification. For reasons of longevity, it is important that the scheme is ultimately owned and operated by industry, rather than by government.

11. What specific market incentives or regulatory changes should Government consider?

While the suggested STM scheme is ultimately self-funding, financial assistance is required for the next phases required to launch, administer and market the scheme; and to maintain and update the scheme as IoT and technologies evolve. Our thesis is that through the STM scheme, government, industry and the community will contribute to building a more resilient and secure national IoT infrastructure. Further details of the STM scheme are contained in the body of our submission.

12. What needs to be done so that cyber security is 'built in' to digital goods and services?

The STM scheme we propose provides a compelling commercial incentive for vendors to build security into their products 'by design', in order to obtain certification and the right to display the Trust Mark. Government can best assist this by introducing purchasing policies to purchase devices and solutions that carry the Trust Mark. Suppliers will have strong incentives to participate to win government supply contracts, and this will raise awareness amongst the wider community.

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

IoTAA strongly agrees If consumers continue to make purchasing decisions based on price or features alone with little to no regard for cyber security, privacy or safety concerns, then cyber incidents will only accelerate, particularly as IoT eco-systems proliferate. Consumers and procurement departments and agencies need to be empowered to make informed decisions and ask critical cyber security, safety and privacy questions, which in turn are addressed by the IoTAA demand side security awareness guide.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

The STM scheme we propose will, by its very design, create an increased consumer focus on IoT security, which will drive Australian and international vendors to create cyber secure products for the Australian market. Australian and international vendors who have obtained the Trust Mark will market their products to consumers using it. This will raise awareness with retailers, who will also promote products carrying the Trust Mark. As the scheme gains momentum, consumers (as well as businesses and government) will seek products and services carrying the Trust Mark. This in turn will send strong signals to other vendors of IoT products and services to build in security into their products and practices, apply for certification under the STM scheme, and to advertise their security compliance as a competitive advantage.

25. Would you like to see cyber security features prioritised in products and services?

IoTAA cannot understate the importance of ensuring appropriate cyber security features are present in *all* IoT devices and solutions. IoT is a key enabler of the fourth industrial revolution that enables us to capture data from a massive array of physical world scenarios for processing in the digital world. It is a fundamental requirement for the future evolution of our economy, allowing us to make more informed and accurate decisions in quicker timeframes to reduce cost, improve performance and reduce our impact on the environmental. At a consumer level, IoT is entering every facet of our lives, from medical/health devices and wearables to smart homes.

Cyber-attacks on these devices and systems can have wide-ranging consequences from disruption to business and customers, financial consequences arising from lost revenue or productivity, through to reputational damage. In the consumer space, consequences range from privacy violations through to our physical security.

We need to do more than simply prioritising security features in IoT products and services; we need to ensure they are included 'by design' at the outset to product development. A voluntary accreditation scheme will facilitate this by providing compelling commercial incentives to vendors and industry participants.