The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
PO Box 289
North Sydney NSW 2059
Australia
ABN 76 369 958 788

26 February 2020

Cyber Security Strategy & Governance Team
Strategy Governance & Industry Branch | Cyber Security Policy Division
Department of Home Affairs
Email: iot.policy@homeaffairs.gov.au

Dear Sir/Madam

DRAFT CODE OF PRACTICE: SECURING THE INTERNET OF THINGS FOR CONSUMERS

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the proposed voluntary *Draft Code of Practice: Securing the Internet of Things for Consumers* (Draft Code of Practice) by the Department of Home Affairs (Department).

1. Introduction

Ai Group's membership comes from a broad range of industries and includes businesses of all sizes. Industry is increasingly characterised by the use of networked systems and the embedding of digital capabilities and communications in all processes, products and services, which some label as part of the Fourth Industrial Revolution (or Industry 4.0), and others refer to in part as the Internet of Things (IoT). These include not just "communications businesses" and "IT businesses", but also a wide range of manufacturers, industrial solutions providers and consumer facing businesses whose products and services are increasingly networked and digital.

Our submission is focussed on the implications for the broader cross-section of Australian businesses. Industry recognises the importance of protecting the cybersecurity of Australian businesses and the broader community. Indeed, Ai Group works closely with government and its agencies on improving Australia's cybersecurity. We support the Department's consideration of a voluntary Code of Practice and our submission recommends a number of areas that merit further investigation and consultation.

At this stage, we would like to provide preliminary views. As further consultation is undertaken, there may be additional matters raised.

We would also welcome the opportunity to work closely with policy makers, governments and regulators as the consultation progresses.

2. Understanding the current market for IoT

Ubiquitous smartphones and connected devices in the workplace and at home mean that doing business in an Industry 4.0 world requires strong digital and communications infrastructure, including IoT which is the focus of this consultation, as well as a mix of other technologies such as 5G and the new Wi-Fi 6 wireless standard (also known as IEEE 802.11ax).

The Australian Communications and Media Authority (ACMA) considers IoT is now mainstream, with greater cost efficiency likely to drive further IoT adoption.[1] Despite these positive expectations, challenges remain for promoting the business value of IoT. According to Australian Bureau of Statistics (ABS) data, more than 60% of businesses did not see any value in IoT.[2] IoT was more likely to be valued by larger businesses and in industries such as mining, retail trade, transport, postal, warehousing, information media and telecommunications.

[1] ACMA, "Communications Report 2017-18" (Report, February 2019), p. 40.
[2] ABS, 8167.0 – Characteristics of Australian Business, 2017-18.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

It is fair to say that substantial progress has been made by businesses in embracing Industry 4.0, whether under that name or others. In our recent report, *The Fourth Industrial Revolution: Australian businesses in transition*, we highlighted companies that are punching above their weight, doing amazing things with new technology and leading the way for others.[3] But there remains a gap between leaders that are digitally enabled and others who are not.

Therefore, it is important in this regard for governments and industry to work together to close the gap in promoting the real business value of IoT, as well as other technologies, to encourage business to adopt greater digital enablement of production and distribution.

3. The roles of regulation, standards and education

Ai Group welcomes the Department's intent for the Draft Code of Practice to remain voluntary at this stage. We believe this approach will create a flexible environment for all stakeholders to shape and implement best practices in a collaborative manner.

This is in contrast to some recent areas of regulation in response to emerging technology, where we have been alarmed by disproportionately heavy-handed interventions that seek to eliminate some forms of security risk, for example, rather than manage them, while ignoring the implications and costs to innovation and the economy. Such measures not only add costs to international business, but risk curtailing innovation and limiting the benefits of digitalisation to businesses and their customers.

For example, the *Telecommunications and other Legislation Amendment (Assistance & Access) Act 2018* (Cth) was rushed through Australian Parliament at the end of 2018 without full consideration of the impact that this could create for a broad range of stakeholders. This has led to unintended consequences, including Australia's image overseas in relation to trust in Australian products and services, and concern that the legislation could lead to the weakening of existing cyber security of businesses and its customers.[4]

Regulation has a clear role in addressing reasonable public concerns, for instance around security, safety, privacy and the environment. But there are also often alternative approaches to the regulatory "stick", including consultation and dialogue, codes of practice, standards, transitional support and education.[5] Regulatory barriers should only be introduced where there are clear net community benefits that are supported by substantiated evidence.

Further, we support a security-by-design approach supported by principles, with the ultimate objective of protecting Australia's cyber security. In this context, governments should reinvigorate and promote best practice regulation initiatives, by taking into account existing business practices and study global best practices in regulation and business support that encourage – rather than inhibit – innovation and productivity.

---

[3] Ai Group, *The Fourth Industrial Revolution: Australian businesses in transition* (Report, August 2019), Link: https://cdn.aigroup.com.au/Reports/2019/AiGroup_Fourth_Industrial_Revolution_Report.pdf.

[4] Joint submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS), *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)* (Submission No. 23, July 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions; Joint submission to the Independent National Security Legislation Monitor (INSLM), *Review of the TOLA Act* (Submission No. 15, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Ai Group submission to the INSLM, *Review of the TOLA Act* (Submission No. 12, September 2019), Link: https://www.inslm.gov.au/submissions/tola; Australian Strategic Policy Institute (ASPI), *Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018* (December 2018), p. 3.

[5] We discuss in more detail about the role of regulation, standards and education with respect to cyber security in our submission to the Department's 2020 Cyber Security Strategy. Link: https://cdn.aigroup.com.au/Submissions/Technology/2020_Aust_Govt_Cyber_Security_Strategy_Discussion_Paper_1Nov_2019.pdf.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

In this regard, we understand that the Department's Draft Code of Practice may have been modelled on the UK's version.[6] While we support consideration of the UK's approach, it is also important to consider its appropriateness in the Australian context.

For instance:

- In the Department's consideration of a Code of Practice, it is not clear whether consideration has been given to the effectiveness of existing industry and internal business practices in Australia. For example, one manufacturing member has tested their IoT system against a global reference, the Open Web Application Security Project (OWASP), which includes top ten things to avoid relating to security in IoT systems.[7]

- The specific products and services targeted in the Draft Code of Practice may be supplied to the Australian consumer market from regions overseas, which might differ from the UK market. It is important to consider the relevant best practices that have been adopted from originating countries that supply products and services to the Australian market. Input from other government agencies already engaged internationally on promoting cyber security development may be of valuable assistance. These include the Australian Ambassador for Cyber Affairs and AustCyber.

- There is an opportunity to promote relevant existing cyber security standards and explain how they apply to products, services and supply chains. For instance, there are international forums such as ISO/IEC and NIST that have developed standards applicable to security-by-design, which appear to be missing from the Department's considerations. These include:

    - ISO/IEC:
        - ISO/IEC 27000 series of standards
        - ISO 31000:2018 *Risk Management*
        - ISO/IEC 27701:2019 *Security Techniques*

    - NIST:
        - NISTIR 8228 *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (Jun 2019)
        - Draft NISTIR 8267 *Security Review of Consumer Home Internet of Things (IoT) Products* (Oct 2019)
        - Draft NISTIR 8259 *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline* (Jan 2020)
        - Draft NIST SP 800-53 Revision 5 *Security and Privacy Controls for Information Systems and Organizations* (Aug 2017)

In addition, businesses and individuals still need to be better informed about good cyber security hygiene. Businesses are also consumers. Raising cyber awareness through education and training will be key to helping consumers understand how to protect their data. This is an area where support from Government and industry can play an important role.

Ai Group recommendation: In reviewing its proposed Draft Code of Practice, the Department should take into consideration:

- ***The effectiveness of existing industry and internal business practices that address cyber security.***

[6] UK Government, *Code of Practice for Consumer IoT Security* (October 2018), Link: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security.

[7] The objective of OWASP is "to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies". Link: https://owasp.org/www-project-internet-of-things/.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

- ***Global best practice approaches including from relevant nations that supply products and services to the Australian market, international standards and whether they are suitable in the Australian context.***
- ***A suitable forum such as Standards Australia to consider international standards discussions that impact on a wide range of sectors.***
- ***The role of education to raise awareness about good cyber hygiene amongst business and consumers.***

4. Consumer protection focus

We note that the Department proposes to focus the Draft Code of Practice on consumer products and services.

As mentioned in our submission to the Department's 2020 Cyber Security Strategy, industry clearly has commercial interests in ensuring that their business and customers' transactions are protected. Customer protections are certainly important. When these protections are implemented, it should govern the requirements in the design and implementation of security in products and services that meets an appropriate cyber security standard.

It is worth noting that consumers are currently afforded protections under the Australian Consumer Law and Privacy Act. If a mandatory approach were to be introduced (as opposed to the voluntary approach proposed by the Department), substantiated evidence will be required if there is a view that the current protections are inadequate, supported by proper consultation with relevant stakeholders to properly identify any problems and develop options to address any identified issues.

Ai Group recommendation: With respect to the consumer focus in its proposed Draft Code of Practice, the Department should take into consideration the effectiveness of existing protections under the Australian Consumer Law and Privacy Act.

5. Scope of policy issues

We note that the Department is currently reviewing the 2020 Cyber Security Strategy, which has triggered this separate consultation on IoT cyber security. We also understand that the Department will consider further initiatives through the Strategy. On our part, we have made extensive comments in our submission to this Strategy, covering a broad range of issues relevant to this particular consultation.

In addition, there are interrelated issues to this consultation with other policy activities relating to IoT, privacy and data use, cyber safety and defamation. Some of these issues are being managed by other Government agencies and bodies, and it will be important for the Department to properly coordinate and understand the scope of these issues. Otherwise, there is a risk of overlapping and conflicting issues.

For instance, current policy consultations that may be relevant to the Department's consultation on its Draft Code of Practice include:

- The Parliamentary Joint Committee on Intelligence and Security (PJCIS) and Independent National Security Legislation Monitor (INSLM) reviews relating to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act) – there are concerns about the potential negative impact of this Act on cyber security and privacy of products and services, as discussed above.[8]

[8] See above n 4.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

- The ACCC's Digital Platforms Inquiry – Government's response to this Inquiry includes policy reforms in the area of privacy and data regulation.[9]

- The Department of Infrastructure, Transport, Regional Development and Communications (DITRDC) consultation on a new Online Safety Act – we have recommended that the DITRDC clearly outline how its online safety proposals will fit with other relevant Government consultations including the 2020 Cyber Security Strategy.[10]

- The Standing Committee on Communications and the Arts Inquiry into 5G in Australia – while cyber security has been excluded from this Inquiry, there are interrelated considerations with respect to the operation of 5G and IoT.[11]

- Treasury's consultation on Improving the Effectiveness of the Consumer Product Safety System – insofar as the Department's Draft Code of Practice relates to the consumer, cyber security may also fall under the scope of Treasury's consultation if it leads to consumer safety issues.[12]

- The Australian Human Rights Commission's (AHRC) consultation into Human Rights and Technology – as the title suggests, the AHRC are exploring the impact on humans as it relates to emerging technologies.[13]

Ai Group recommendation: Given the potential overlap between the Department's Draft Code of Practice and other public consultations and initiatives, the Department should clearly outline how its Draft Code of Practice will fit with other relevant consultations and initiatives.

6. Specific principles proposed in Draft Code of Practice

We have received the following member feedback concerning specific principles that the Department has included in its Draft Code of Practice – these require further review:

- Principle #3 ("Keep software securely updated"): Some companies may already implement the automatic update recommendation as a best practice in their products and services. However, there may be circumstances where users will need to take affirmative steps to deploy a security update e.g. an operating system update that includes a security update in amongst other changes. Clarity should also be provided around expectations specifically on critical security updates.

- Principle #5 ("Ensure that personal data is protected"): This proposal should also consider including regular reviews on who has access to data and personal information, and to limit access to confidential and sensitive information.

- Principles #6 ("Minimise exposed attack surfaces") and #7 ("Ensure communication security"): Depending on how aggressively the TOLA Act is invoked by law enforcement, security and intelligence agencies, it may be difficult to meet these principles.

---

[9] Ai Group submission to ACCC, *Digital Platforms Inquiry Final Report* (September 2019), Link: https://cdn.aigroup.com.au/Submissions/Technology/AiGroup_submission_Digital_Platforms_Inquiry.pdf
[10] Ai Group submission to Commonwealth Department of Infrastructure, Transport, Regional Development & Communications, *Consultation on a new Online Safety Act* (February 2020), Link: https://cdn.aigroup.com.au/Submissions/Technology/New_Online_Safety_Act_Proposals_21Feb_2020.pdf.
[11] Ai Group submission to Standing Committee on Communications and the Arts, *Inquiry into 5G in Australia* (Submission No. 356, November 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/House/Communications/5G/Submissions
[12] Commonwealth Treasury, *Improving the Effectiveness of the Consumer Product Safety System*, Link: https://consult.treasury.gov.au/market-and-competition-policy-division-internal/main-consultation.
[13] AHRC, *Discussion Paper on Human Rights and Technology*, Link: https://tech.humanrights.gov.au/consultation.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

- Principle #9 ("Make systems resilient to outages"): This principle may require support capabilities being implemented in the broader network ecosystem to monitor devices for resilience, availability and end-to-end observability, and to deploy self-healing measures in case of observed failure.

- Principle #11 ("Make it easy for consumers to delete personal data"): The scope of this principle should be broadened to contemplate de-identification rather than simply deletion – de-identification is important for business retention of data.[14] As the principle currently reads, the scope could be misinterpreted or taken beyond cases of personal device transfer of ownership.

- Principle #12 ("Make installation and maintenance of devices easy"): This principle may require support maintenance procedures that are executed by taking the device out of service and being augmented by a similar capability.

Ai Group recommendation: The Department should consider our specific issues raised in relation to Principles 3, 5, 6, 7, 9, 11 and 12 of the Draft Code of Practice.

If you would like clarification about this submission, please do not hesitate to contact me or our Digital Capability and Policy Lead Charles Hoang (02 9466 5462, charles.hoang@aigroup.com.au).

Yours sincerely,

Peter Burn
Head of Influence and Policy

[14] During the ACCC's Digital Platforms Inquiry, Ai Group identified a number of issues relating to the ACCC's proposal for erasure of personal information, including the obligations of data retention and de-identification of data that would conflict with the ACCC's proposal. We therefore recommended that more work needs to be undertaken on considering the consequences and material benefit of allowing individuals to request that personal data be deleted. See above n 9.