www.accan.org.au
info@accan.org.au
02 9288 4000

Submission

1 March 2024

Department of Home Affairs
PO Box 25
Belconnen ACT 2616
AusCyberStrategy@homeaffairs.gov.au

Re: 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper

The Australian Communications Consumer Action Network (**ACCAN**) thanks the Department of Home Affairs (**the Department**) for the opportunity to comment on the *2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper* (**the Consultation Paper**).

ACCAN is the peak body that represents consumers on communications issues including telecommunications, broadband, and emerging new services. ACCAN provides a strong unified voice to industry and government as we work towards communications services that are trusted, inclusive and available for all.

ACCAN supports the legislative reforms introduced by the Consultation Paper to address the gaps in the current regulatory frameworks. These reforms include:

- 'Mandating a security standard for consumer-grade Internet of Things (**IoT**) technology to incorporate basic security features by design and help prevent cyber attacks on Australian consumers'.[1]
- 'Creating a no-fault, no-liability ransomware reporting obligation to improve our collective understanding of ransomware incidents across Australia'.[2]
- 'Creating a "limited use" obligation to clarify how the ASD [Australian Signals Directorate] and the Cyber Coordinator use information voluntarily disclosed during a cyber incident, in order to encourage industry to continue to collaborate with the Government on incident response and consequence management'.[3]
- 'Establishing Cyber Incident Review Board to conduct no-fault incident reviews and share lessons learned to improve our national cyber resilience'.[4]
- The Consultation Papers proposed changes to the Security of Critical Infrastructure Act 2018 (**the SOCI Act**).[5]

[1] Australian Government. 2023. Cyber Security Legislative Reforms Consultation Paper. p.7. Available at: https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/cyber-security-legislative-reforms.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid p.30.

ACCAN recommends that:

- Any mandatory security standards developed for consumer IoT devices make mandatory the first six principles of the ETSI EN 303 645 standard (**the ETSI standard**) in addition to making it mandatory that device manufacturers make it easy for consumers to delete personal data.
- ACCAN considers that the Department should ensure that IoT devices conform with the AS EN 301 549 (Accessibility requirements for ICT products & services) standard.[6]
- Mandatory requirements be introduced which ensure that IoT device manufacturers understand and limit the pathways through which their devices may be used to facilitate technology facilitated coercive control (**TFCC**). ACCAN considers that only manufacturers who supply over a certain number of products to the Australian market, subject to further consultation, should have to comply with this mandatory requirement.
- The ACCC be integrated into the regulation and enforcement of mandatory smart device cybersecurity standards.
- A labelling scheme be introduced for smart devices to be covered under any future mandatory smart device standards. ACCAN considers that this should be undertaken through a phased implementation process prior to being made mandatory and regulated by the ACCC. This scheme will inform consumers of the security protections their device offers, fostering genuine competition in the smart device market based on the quality of cybersecurity protections.
- The Department work with the appropriate stakeholders to develop a well-publicised, accessible and timely ransomware reporting hotline or webform to assist small businesses in reporting ransomware instances.
- IoT devices should be designed and manufactured with the needs of people with disability in mind and sold with intuitive and simple accessibility settings set by default.[7]
- 'Device manufacturers should also be required to provide accessible information on data collection practices and the security by design features included in IoT devices, including instructions on how to withdraw consent or delete collected data, so that consumers with disabilities can exercise the same control over their personal information as consumers without disability.'[8]

For ACCAN's extended comments and responses to the Consultation Paper's questions, please see **Attachment A**.

We thank the Department for the opportunity to comment on the Consultation Paper. Should you wish to discuss any of the issues raised in this submission further, please do not hesitate to contact me at: [redacted]

Yours Sincerely,

Con Gouskos

Policy Officer

[6] ETSI. 2021. EN 301 549 V3.2.1 (2021-03) Accessibility requirements for ICT products and services. Available at: https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf.
[7] ACCAN. 2021. Internet of Things Position Paper. p.9. Available at: https://accan.org.au/accans-work/policy-positions/1893-iot-policy.
[8] Ibid.

Attachment A

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

ACCAN considers that smart device manufacturers, distributors and importers should be responsible for complying with a proposed mandatory cyber security standard relating to IoT devices.[9] Device manufacturers are best placed to address the nature of consumer harm caused by IoT devices as they can configure the software and hardware of IoT devices prior to customer interaction with these devices.[10] However, 'given the vast majority of IoT devices are manufactured offshore and are either imported for sale or purchased by consumers directly online, regulatory measures will need to be applicable post-manufacture to capture all devices sold and used by Australian consumers.'[11]

Question 2: Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?

ACCAN would support increasing the number of principles which a minimum standard for consumer grade IoT devices would contain from the three principles proposed in the Consultation Paper.

ACCAN supports the expansion of mandatory principles to include the first six of the 13 principles detailed in the Australian Governments' *IoT Secure-by-Design Guidance for Manufacturers*.[12] Additionally, ACCAN considers that a mandatory requirement for manufacturers to 'make it easy for consumers to delete personal data' is reasonable and incremental change which manufacturers should be required to undertake during device design and manufacture.[13]

A mandatory standard for internet of things devices should make mandatory the following principles:

- No duplicated default or weak passwords.
- Implement a vulnerability disclosure policy.
- Keep software securely updated.
- Securely store credentials.
- Ensure that personal data is protected.
- Minimise exposed attack surfaces.
- Make it easy for consumers to delete personal data.[14]

Additionally, ACCAN notes that as the 13 principles chosen for the UK's voluntary IoT code of practice were listed in order of importance, there is sufficient cause to improve upon the proposed mandatory principles.[15] ACCAN considers that these criteria are of sufficient importance to warrant inclusion in Australian mandatory smart device standards. Improving upon three mandatory principles of a mandatory Iot standard was supported by the World Economic Forum which made

[9] ACCAN. 2021. Internet of Things Position Paper. p.10. Available at: https://accan.org.au/accans-work/policy-positions/1893-iot-policy.
[10] Ibid. p.9.
[11] Ibid. p.4.
[12] Australian Government Australian Signals Directorate. 2023. IoT Secure-by-Design Guidance for Manufacturers. p.1. Available at: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/iot-secure-design-guidance-manufacturers.
[13] Ibid.
[14] Ibid.
[15] ACCAN. 2020. Regulation of Internet of Things Devices to Protect Consumers Summary Report. p.6. Available at: https://accan.org.au/grants/current-grants/1781-regulation-of-internet-of-things-devices-to-protect-consumers.

reference to five 'must haves' of IoT security essentials and principles.[16] The incremental costs experienced by manufacturers adapting to new regulatory settings must be weighed against the material benefits of improved security.

ACCAN considers that ensuring the most practical and comprehensive secure by design principles are established by the government is critical as the 'complexity of security configuration should not be a customer problem' due to the time poor nature of consumers and the sometimes limited digital ability that consumers may possess, which might hinder their understanding of cybersecurity.[17]

Consumers who are not confident in their digital skills and/or have limited digital ability should have confidence that at the outset of the purchase they are receiving some cybersecurity protections from the devices they purchase. This would facilitate a more competitive and effective IoT device market as consumers can place greater trust in devices they purchase, with the knowledge they are covered by mandatory regulations.

Research from the Good things Foundation noted that:

- 20% of people said they felt overwhelmed with constant changes in technology with 16% stating they are not able to keep up.[18]
- Two thirds of those surveyed were not confident in their ability to stay up to date with the constant changes in technology, with 1 in 4 saying they need more support to keep up.[19]

Additionally, a survey of smart home device owners in 21 countries (not including Australia) by Arlington Research for cybersecurity company Kaspersky noted that:

- 34% of respondents believe that simply buying devices from trusted manufacturers is enough for digital protection.[20]
- 35% of people have heard of or know the terminology 'internet of things'.[21]
- 56% are mostly worried about their internet-connected home security use and protection when it comes to smart devices such as baby or pet monitoring cameras being used to spy on them or being hacked over Wi-Fi.[22]
- 56% of those who own a smart home gadget believe they are responsible for the protection of their devices.[23]

'Technology-facilitated abuse is estimated to involve 8% to 48% of all DFV cases, with 27% of children in Australia experiencing technology-facilitated DFV.'[24] Additionally, 98 percent of Australian domestic abuse support workers report they have clients who have experienced technology-facilitated abuse.[25] If not securely protected, the granular data collected by IoT devices, including location data, can be used by abusers to perpetrate TFCC. It is critical that 'the risk of tech

[16] ACCAN. 2020. Regulation of Internet of Things Devices to Protect Consumers Summary Report. p.3 Available at: https://accan.org.au/grants/current-grants/1781-regulation-of-internet-of-things-devices-to-protect-consumers.
[17] Cybersecurity and Infrastructure Security Agency. 2023. Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and -Default. p.6. Available at: https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf.
[18] Good Things Foundation. 2023. Report: Australian attitudes to getting online. Available at: https://www.goodthingsfoundation.org.au/news/report-australian-attitudes-to-getting-online/.
[19] Good Things Foundation. 2023. Report: Australian attitudes to getting online. Available at: https://www.goodthingsfoundation.org.au/news/report-australian-attitudes-to-getting-online/.
[20] Kaspersky. 2023. IoT Survey Report. Available at: https://www.kaspersky.com/blog/iot-survey-report-2023/.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] ACCAN. 2023. Domestic and Family Violence Policy Position. p.1. Available at: https://accan.org.au/accans-work/policy-positions/2253-domestic-and-family-violence.
[25] ACCAN. 2021. Internet of Things Position Paper. p.10. Available at: https://accan.org.au/accans-work/policy-positions/1893-iot-policy.

abuse must be incorporated into risk assessments and safety planning processes' of IoT device manufacturers.[26] Requiring IoT device manufacturers to consider the consumer harm facilitated through their devices would help limit consumer vulnerabilities and improve consumer confidence in the IoT market. IoT devices are 'inherently designed based on the assumptions that all of their users trust each other' which may leave consumers vulnerable to avenues of abuse if device manufacturers do not account for the possibility of TFCC in the design and manufacture of their products.[27]

ACCAN recommends the expansion of any mandatory standard introduced for IoT devices sold in Australia to include a requirement for IoT device manufacturers to examine and limit the pathways in which perpetrators of TFCC may utilise the device to perpetrate harm. ACCAN considers that only manufacturers who supply over a certain number of products to the Australian market be subject to this requirement.

Question 3: What alternative standards, if any, should the Government consider?

'Many people with disability encounter barriers in accessing Digital Communication Technologies'.[28] ACCAN considers that the Department should ensure that IoT devices conform with the AS EN 301 549 (Accessibility requirements for ICT products & services) standard.[29] Additionally, online and app interfaces for IoT devices should conform with the latest version of Web Content Accessibility Guidelines at AA level at a minimum. This ensures people with disability have equal access to IoT devices including security features and interfaces.

Question 4: Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?

ACCAN considers that a broad definition subject to exceptions is appropriate to be used to define the smart devices that are subject to an Australian mandatory standard. ACCAN considers that the Department or Minister for Home Affairs should have the ability to add device categories to the definition via regulation. ACCAN considers that the government should have a timely mechanism to update what devices are subject to mandatory standards.

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

ACCAN notes that due to cross sector legislative development in medical devices, computers and connected vehicles it is reasonable to exclude them from a mandatory standard. While this is a reasonable exemption, ACCAN has concerns that due to the nature of data collected by medical devices and computers, that consumers may lack protections in the interim, while sector specific legislation is being developed. ACCAN would support the Department taking this lapse in cybersecurity protection into account when defining the devices subject to an Australian mandatory standard. ACCAN considers that the regulation surrounding the types of smart devices that should be covered by a mandatory cyber security standard should be flexible and allow for developments in

[26] Tanczer, L, Lopez Neira, I, Parkin, S, Patel, T, Danezis . 2018. Gender and IoT Research Report. p.6. Available at: https://www.ucl.ac.uk/computer-science/research/research-groups/gender-and-tech/gender-and-iot#Research.
[27] Ibid p.4.
[28] The Australian Human Rights Commission noted many limits of the limits on functional accessibility of digital communications devices, including Internet of Things devices. Australian Human Rights Commission. 2021. Final Report: Human Rights and Technology. p.137. Available at: https://humanrights.gov.au/our-work/technology-and-human-rights/publications/final-report-human-rights-and-technology.
[29] ETSI. 2021. EN 301 549 V3.2.1 (2021-03) Accessibility requirements for ICT products and services. Available at: https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf.

the smart device market to occur without decreasing the protections afforded to consumers. If required, any changes to the types of smart devices covered by a mandatory cyber security standard should be subject to consultation.

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

ACCAN considers that 12 months is an appropriate timeframe for industry to adjust to new cyber security requirements.

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

ACCAN considers that in designing an appropriate regulatory and enforcement model, that the ACCC should cooperate with the Department. Additionally, ACCAN considers that the ACCC and the Department cooperating on the enforcement of mandatory IoT standards is an appropriate solution with regard to the enforcement of mandatory consumer IoT device standards. Leveraging the ACCC's significant expertise and purview of the Australian economy would improve regulatory and compliance outcomes for consumers. Implementing proposed mandatory standards would be more effective through cooperation with the ACCC and provide a suitable framework for monitoring a mandatory cybersecurity standard for smart devices.

Question 11: Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

ACCAN considers that there is merit in aligning the ransomware reporting obligation to the Australian Tax Office small business threshold. Small businesses who suffer from ransomware attacks should be greater supported in their reporting of ransomware attacks. Establishing a service similar to a hotline or webform would assist small businesses in reporting ransomware attacks. Facilitating small business reporting of ransomware incidents should be done in cooperation with police and other authorities which small businesses are likely to be in contact with after an incident has occurred. To ensure that small businesses are supported in voluntary ransomware reporting, the Department should ensure that ransomware reporting resources are well publicised alongside other resourced used by small business and are accessible, timely and free.